

MOBILEIRON, INC.
Plan de protección de datos
(versión del 15 de mayo de 2018)

Este Plan de protección de datos, incluidos los Anexos (en conjunto, el “**DPA**”), complementa, integra y forma parte del Contrato con el cliente entre el Cliente y MobileIron (el “**Contrato**”). En caso de surgir un conflicto entre una disposición de este DPA y una disposición del Contrato, prevalecerá la disposición del DPA.

1. Definiciones.

- a. En el caso de los términos con mayúscula inicial que no estén definidos en este DPA, se aplicará la definición presente en el Contrato.
- b. “**Datos de cliente**” hace referencia a todos los Datos personales proporcionados a MobileIron por el Cliente o en su nombre a través del uso de los Servicios en línea; dicho alcance queda a criterio exclusivo del Cliente.
- c. “**Documentación**” hace referencia a las notas de versión, guías de implementación u otra documentación técnica publicada de forma escrita o electrónica sobre la Solución de MobileIron que MobileIron brinda al Cliente o pone a su disposición.
- d. “**Usuario final**” hace referencia al individuo que utiliza una Solución de MobileIron.
- e. “**Solución de MobileIron**” hace referencia a un Software o Producto de SaaS, o a ambos.
- f. “**Servicios en línea**” hace referencia a los servicios alojados por MobileIron que el Cliente adquiere en virtud del Contrato como servicios independientes o como parte de una plataforma o aplicación de MobileIron. El término Servicios en línea no incluye MobileIron Government Cloud, pruebas gratuitas, servicios de una marca distinta que operan fuera del control de MobileIron, o software y servicios proporcionados mediante una licencia o términos de suscripción diferentes. Los Servicios en línea no incluyen el Software, pero pueden incluir cualquier servicio alojado por MobileIron que sea necesario para el funcionamiento integral del Software.
- g. “**Orden**” hace referencia a la orden de compra, anexo del producto, o documento de la orden entre el Cliente y un distribuidor autorizado (o entre el Cliente y MobileIron si la compra se realiza directamente desde MobileIron) en la que se identifica la Solución de MobileIron o los servicios vendidos u otorgados bajo licencia, así como cualquier suscripción o parámetro de licencia vigente (p. ej., la cantidad de suscripciones).
- h. “**Datos personales**” hace referencia a cualquier información ingresada en los Servicios en línea relacionada con (i) una persona física identificada o identificable y (ii) una entidad jurídica identificada o identificable en donde dicha información se protege del mismo modo que los Datos personales o la información de identificación personal, conforme a las leyes vigentes de protección de datos. Una persona física identificable es una persona que puede ser identificada, de forma directa o indirecta, específicamente a través de un identificador como el nombre, el número de identificación, los datos de ubicación, un identificador en línea o uno o más factores específicos a la identidad física, psicológica, genética, mental, económica, cultural o social de dicha persona física.
- i. “**Producto de SaaS**” hace referencia a los servicios que se encuentran disponibles al acceder y usar el software alojado por MobileIron, lo que incluye cualquier Documentación.
- j. “**Incidente de seguridad**” hace referencia al acceso ilegal a los Datos personales almacenados en los equipos o las instalaciones de MobileIron, así como al acceso no autorizado a dichos equipos o instalaciones que genere la pérdida, divulgación o alteración de los Datos personales.
- k. “**Software**” hace referencia a la versión de código objeto de los programas informáticos de propiedad exclusiva de MobileIron que este último haya puesto a disposición del Cliente para su descarga (lo que incluye el uso relacionado con cualquier Producto de SaaS), incluida la Documentación y las Actualizaciones.
- l. “**Subprocesadores**” hace referencia a otros procesadores utilizados por MobileIron para procesar los Datos personales en nombre del Cliente. Para evitar cualquier duda, las instalaciones de coemplazamiento para los centros de datos de MobileIron no se consideran Subprocesadores.
- m. “**Datos de soporte**” hace referencia a todos los Datos personales, además de los Datos de cliente, proporcionados a MobileIron por el Cliente o en su nombre (o que MobileIron obtiene a través de los Servicios en línea previa autorización del Cliente) en virtud de un acuerdo con MobileIron para recibir soporte técnico o servicios de asesoramiento para los Servicios en línea o el Software incluidos en el Contrato; dicho alcance queda a criterio exclusivo del Cliente.
- n. “**Plazo**” hace referencia al plazo de la suscripción del Producto de SaaS o de la licencia del Software, conforme a lo especificado en la Orden relevante, el cual comienza en el momento en que MobileIron pone a disposición las credenciales de acceso y uso del Producto de SaaS o habilita la descarga del Software.
- o. “**Actualizaciones**” hace referencia a las correcciones, actualizaciones, mejoras, parches u otras modificaciones o adiciones implementadas por MobileIron en un Software específico.

2. Cumplimiento de las leyes.

- a. **Mobilelron.** Mobilelron debe cumplir todas las leyes y reglamentaciones vigentes para la prestación de los Servicios en línea, incluida la ley de notificación de violaciones de seguridad. Todos los Incidentes de seguridad están sujetos a la Sección 7. Mobilelron no se responsabiliza del cumplimiento de las leyes o reglamentaciones vigentes para el Cliente o la industria del Cliente que no rijan de manera general para los proveedores de servicios de tecnología de la información. Mobilelron no determina si los Datos de cliente o los Datos de soporte incluyen información sujeta a leyes o reglamentaciones específicas.
- b. **Cliente.** El Cliente debe cumplir todas las leyes y reglamentaciones vigentes para el uso de los Servicios en línea, incluidas las leyes relacionadas con la privacidad, los Datos personales, los datos biométricos, la protección de datos y la confidencialidad de las comunicaciones. El Cliente es responsable de (i) implementar y preservar las medidas de seguridad y de protección de privacidad correspondientes a los componentes y las configuraciones de las Soluciones de Mobilelron que controla o proporciona el Cliente (incluidos los dispositivos registrados con una Solución de Mobilelron), (ii) determinar si los Servicios en línea son apropiados para almacenar y procesar información sujeta a leyes o reglamentaciones específicas, (iii) utilizar los Servicios en línea conforme a las obligaciones reglamentarias y legales del Cliente, (iv) efectuar divulgaciones, obtener consentimientos y brindar accesos, opciones y otros derechos vigentes a los usuarios finales respecto al procesamiento de Datos personales requeridos conforme a las leyes, reglamentaciones o normas vigentes, y (v) responder las solicitudes de terceros relacionadas con el uso de los Servicios en línea por parte del Cliente. Para mayor claridad, la implementación, la configuración y el uso de los Servicios en línea por parte del Cliente, lo que incluye cualquier otro producto o servicio ofrecido por Mobilelron e integraciones de terceros, puede influir en el alcance y la forma de procesar los Datos personales.

3. Uso de datos.

- a. **Datos de cliente y Datos de soporte.** Los Datos de cliente se utilizarán solo para brindar Servicios en línea (incluidos usos compatibles) al Cliente y, por ejemplo, implementar y proporcionar Soluciones de Mobilelron y sus características y servicios asociados, brindar soporte al Cliente y asistir al Cliente para evitar o solucionar problemas técnicos o de servicio. Los Datos de soporte solo se utilizarán para brindar soporte (incluidos usos compatibles) al Cliente y, por ejemplo, solucionar problemas recurrentes e introducir mejoras para el soporte o los Servicios en línea. Mobilelron no utilizará los Datos de cliente, los Datos de soporte ni la información derivada de estos para fines publicitarios o fines comerciales similares. En lo que respecta a las partes, el Cliente se reserva todos los derechos sobre los Datos de cliente y los Datos de soporte. Mobilelron no posee ningún derecho sobre los Datos de cliente ni los Datos de soporte, excepto los derechos que el Cliente otorga a Mobilelron para brindarle Servicios en línea o soporte. Este párrafo no afecta los derechos de Mobilelron sobre las Soluciones de Mobilelron adquiridas por el Cliente.
- b. **Datos agregados y sin referencias personales.** Mobilelron recolecta, analiza y utiliza datos agregados, anonimizados o sin referencias personales e información relacionada (como el uso del producto o de una característica, las métricas o los metadatos del dispositivo o el uso de la aplicación móvil) conforme a lo dispuesto por la ley vigente para agilizar los estudios de mercado, el desarrollo o la optimización del producto, los análisis del uso del producto y los servicios de soporte y mantenimiento. Mobilelron puede utilizar, almacenar o divulgar dichos datos o materiales derivados de esta información siempre que dicha información no pueda identificar ni atribuirse a ningún individuo.

4. **Servicios profesionales y datos relacionados.** Los servicios profesionales no se consideran Servicios en línea, y la información proporcionada a Mobilelron durante la contratación de servicios profesionales está protegida por los términos de confidencialidad de este Contrato. El resto de este DPA no se aplica a dicha información, a menos que se trate de Datos personales sujetos a la Sección 14 de este DPA.

5. Confidencialidad de los datos

- a. Mobilelron no divulgará los Datos de cliente ni los Datos de soporte fuera de Mobilelron o de sus filiales y dependencias controladas excepto (i) cuando lo indique el Cliente, (ii) según lo descrito en el Contrato, o (iii) conforme a lo requerido por ley.
- b. Al recibir una solicitud o demanda de Datos de cliente o Datos de soporte por parte de un tercero, Mobilelron notificará de inmediato al Cliente, excepto en los casos prohibidos por ley. Mobilelron rechazará la solicitud, a menos que su cumplimiento sea obligatorio por ley. Si la solicitud es válida, Mobilelron intentará redirigir al tercero para que este envíe la solicitud o demanda directamente al Cliente.
- c. Mobilelron no proporcionará a terceros lo siguiente: (i) acceso directo, indirecto, generalizado o ilimitado a los Datos de cliente o los Datos de soporte; (ii) códigos de encriptación utilizados para asegurar los Datos de cliente o los Datos de soporte, o la capacidad de descifrar dicha encriptación; o (iii) acceso a los Datos de cliente o los Datos de soporte si Mobilelron es consciente de que los datos se utilizarán para otros fines no mencionados en la solicitud del tercero.

6. **Seguridad.** Mobilelron se compromete a ayudar a proteger la seguridad de los Datos de cliente. Mobilelron ha implementado, preservará y dará cumplimiento a las medidas técnicas y organizativas apropiadas destinadas a proteger los

Datos de cliente y evitar el acceso, la divulgación, la alteración, la pérdida o la destrucción accidental, ilegal o no autorizada de dichos datos. En ese sentido, MobileIron ha implementado, preservará y dará cumplimiento, en los sistemas informáticos que alojan los Servicios en línea o que se comunican con estos, a las medidas de seguridad descritas en la siguiente tabla, las cuales, junto con los acuerdos de seguridad del Contrato y sin perjuicio para las obligaciones del Cliente establecidas en la Sección 2.b, representan la única responsabilidad que tiene MobileIron respecto a la seguridad de los Datos de cliente. MobileIron puede actualizar o modificar periódicamente las medidas de seguridad descritas a continuación si dicha actualización o modificación no menoscaba la seguridad general.

Categoría del control de seguridad	Descripción
1. Gestión	<ul style="list-style-type: none"> a. Asignar a un individuo o grupo de individuos los roles adecuados para el desarrollo, la coordinación, la implementación y la gestión de las protecciones administrativas, físicas y técnicas de MobileIron diseñadas para proteger la seguridad, confidencialidad e integridad de los Datos personales b. Emplear personal de seguridad lo suficientemente capacitado, calificado y experimentado para cumplir las funciones relacionadas con la seguridad de la información.
2. Controles de acceso	<ul style="list-style-type: none"> a. Identificar al personal o las categorías del personal que, por motivos relacionados con sus funciones y responsabilidades comerciales, necesitan acceder a los Datos personales, los sistemas relevantes y las instalaciones de la organización b. Preservar los controles diseñados para restringir el acceso a los Datos personales, los sistemas relevantes y las instalaciones que alojan los sistemas al personal autorizado c. Revisar los derechos de acceso del personal de forma periódica y regular d. Preservar los controles de acceso físico a las instalaciones que contienen sistemas, lo que incluye el uso de llaveros a control remoto o tarjetas de acceso emitidos para el personal de MobileIron según corresponda e. Preservar las políticas que exigen la eliminación del acceso físico y electrónico a los sistemas y Datos personales luego del despido de un empleado f. Controles de acceso diseñados para autenticar usuarios y restringir el acceso a los sistemas g. Políticas que restringen el acceso a las instalaciones de centros de datos que alojan sistemas al personal aprobado del centro de datos y el personal aprobado y limitado de MobileIron. h. Preservar los procesos de autenticación de acceso doble para los empleados de MobileIron que posean derechos de acceso administrativos para los sistemas
3. Evaluación de riesgos	<ul style="list-style-type: none"> a. Realizar evaluaciones de riesgo periódicas diseñadas para analizar los riesgos existentes en la seguridad de la información, identificar posibles nuevos riesgos y evaluar la eficacia de los controles de seguridad existentes b. Preservar los procesos de evaluación de riesgos diseñados para evaluar las probabilidades de que surjan riesgos y los posibles impactos significativos que generarían dichos riesgos c. Documentar las evaluaciones de riesgos formales d. Revisar las evaluaciones de riesgos formales a cargo del personal gerencial apropiado
4. Clasificación, conservación y eliminación de datos	<ul style="list-style-type: none"> a. Preservar las políticas que establecen la clasificación de datos según la criticidad y sensibilidad de los datos b. Preservar las políticas que establecen la conservación de datos y los requisitos de destrucción segura
5. Verificación de antecedentes del personal	Preservar las políticas que exigen la verificación razonable de los antecedentes de los empleados nuevos que accederán a los Datos personales o sistemas relevantes, conforme a la ley local
6. Capacitación y formación del personal	Capacitar de forma regular y periódica al personal respecto a los controles y las políticas de seguridad de la información relevantes para las responsabilidades comerciales y los roles desempeñados dentro de la organización
7. Gestión y supervisión de proveedores	Revisar periódicamente los informes de evaluación de seguridad disponibles de los proveedores que alojan los sistemas para evaluar sus controles de seguridad y analizar las excepciones establecidas en dichos informes
8. Supervisión, detección de intrusiones y respuesta a incidentes	<ul style="list-style-type: none"> a. Supervisar el acceso, la disponibilidad, la capacidad y el rendimiento de los sistemas y de los cortafuegos, los registros del sistema y el tráfico del servidor relacionados utilizando diversos software y servicios de supervisión b. Preservar la detección/prevenición de intrusiones (IDS/IPS) en los sistemas localizados en los Estados Unidos, a los cuales se puede acceder directamente a través de un distribuidor de carga c. Preservar los procedimientos de respuesta a incidentes para identificar e informar los incidentes de seguridad y actuar en consecuencia d. Crear un equipo interdisciplinario de repuesta a incidentes de seguridad

Categoría del control de seguridad	Descripción
9. Encriptación	a. Encriptar los Datos personales en HTTPS mediante el protocolo SSL al momento de efectuar las transmisiones desde aplicaciones web, y aplicar una encriptación mínima de 128 bit para dicho tráfico b. Las encriptaciones de los datos de producción y las copias de seguridad se realizan en una ubicación remota
10. Cortafuegos	Preservar los cortafuegos del hardware y software para proteger los sistemas
11. Controles de cambios	a. Asignar la responsabilidad relacionada con la seguridad, los cambios y el mantenimiento del sistema b. Examinar, evaluar y autorizar los componentes principales del sistema antes de su implementación
12. Seguridad física	Usar instalaciones de coemplazamiento y centros de datos gestionados para el alojamiento de sistemas que incluyan lo siguiente: a. múltiples niveles de seguridad física, lo que incluye control interno y externo las 24 horas del día, los 365 días del año, y el registro de los accesos b. sistemas de alimentación ininterrumpida (UPS), generadores y sistemas de refrigeración
13. Administración y disponibilidad del sistema	a. Usar el protocolo de puerta de enlace de frontera (BGP) con al menos dos ISP de nivel superior diseñados para preservar el acceso a Internet en las instalaciones de centros de datos que alojan los sistemas b. Preservar los procesos de parcheo de seguridad en los sistemas que documentan los niveles de parcheo actuales, determinan la disponibilidad de los parches y establecen procesos para evaluar e implementar los parches

7. **Notificación de incidentes de seguridad**

- a. Si MobileIron detecta un Incidente de seguridad, realizará inmediatamente lo siguiente: (i) notificará el Incidente de seguridad al Cliente; (ii) investigará el Incidente de seguridad y proporcionará al Cliente información detallada sobre este; (iii) implementará medidas razonables para mitigar los efectos y minimizar los daños causados por el Incidente de seguridad. MobileIron asignará y capacitará al personal para que pueda (i) comunicarse con el Cliente con respecto a los problemas de seguridad de los Datos personales; (ii) recibir notificaciones de Incidentes de seguridad; (iii) notificar dichos Incidentes de seguridad al Cliente conforme a la Sección 7 y la ley vigente; y (iv) coordinar la respuesta y las medidas correctivas de MobileIron para este Incidente de seguridad. La obligación de MobileIron de notificar el incidente y brindar una respuesta no implica un reconocimiento por parte de MobileIron de ninguna falta o responsabilidad respecto al Incidente de seguridad.
- b. El Cliente debe (i) verificar que los administradores del Cliente posean información de contacto precisa para cada Solución de MobileIron y (ii) notificar inmediatamente a MobileIron cualquier posible uso indebido de sus cuentas o credenciales de autenticación, así como cualquier Incidente de seguridad relacionado con los Servicios en línea.

8. **Ubicación del procesamiento de datos.** Excepto lo descrito en otros puntos del Contrato, los Datos de cliente y los Datos de soporte que MobileIron procese en nombre del Cliente pueden transferirse, almacenarse y procesarse en los Estados Unidos o en cualquier otro país en donde se encuentren las instalaciones de MobileIron o de sus subcontratistas y filiales. En general, MobileIron almacenará los Datos de cliente en la región disponible que (i) haya sido seleccionada por el Cliente (en caso de encontrarse disponible para los Servicios en línea) o (ii) se haya determinado conforme a la información de contacto proporcionada por el Cliente. Si el Cliente decide, a su entera discreción, enviar los Datos de cliente y los Datos de soporte a MobileIron junto con una solicitud de soporte técnico, MobileIron podrá almacenar los Datos de cliente y los Datos de soporte de forma limitada en otras ubicaciones para brindar el soporte solicitado por el Cliente. El Cliente delega a MobileIron la transferencia de los Datos de cliente y Datos de soporte a dicho país, así como su almacenamiento y procesamiento para la prestación de los Servicios en línea.

9. **Conservación de datos.** En todo momento durante el Plazo de los Servicios en línea independientes, el Cliente podrá acceder a los Datos de cliente almacenados en los Servicios en línea y extraer dichos datos, en la medida de lo posible. A excepción de las pruebas gratuitas, MobileIron conservará los Datos de cliente almacenados en los Servicios en línea independientes durante al menos 90 días después de la finalización del Plazo o de la suscripción o licencia relacionada para que el Cliente pueda extraer los datos. Después del período de conservación de 90 días, MobileIron inhabilitará la cuenta del Cliente y eliminará los Datos de cliente.

10. **Personal de MobileIron.** El personal de MobileIron no procesará los Datos de cliente ni los Datos de soporte sin la autorización del Cliente. El personal de MobileIron tiene la obligación de preservar la confidencialidad de los Datos de cliente y los Datos de soporte según lo establecido en este DPA, y esta obligación se mantendrá vigente tras la finalización del acuerdo.

11. **Subcontratistas.** MobileIron podrá emplear subcontratistas, incluidas sus filiales corporativas, para la prestación de servicios limitados o auxiliares en su nombre. Dichos subcontratistas podrán acceder a los Datos de cliente y los Datos de soporte

únicamente para brindar los servicios asignados por MobileIron y no podrán utilizar los Datos de cliente y los Datos de soporte para otros fines. MobileIron será responsable del cumplimiento por parte de los subcontratistas de las obligaciones de MobileIron, las cuales se incluyen en el Contrato. Las Secciones 18 y 19 contienen términos adicionales relacionados con los Subprocesadores.

11. Auditorías y revisiones de seguridad de los Servicios en línea

a. Auditorías. En el caso de los Servicios en línea independientes, MobileIron iniciará, al menos anualmente, una auditoría sobre la seguridad de las computadoras, el entorno informático y los centros de datos físicos utilizados para procesar los Datos de cliente; para realizar esto, MobileIron seleccionará a un tercero calificado e independiente y costeará sus gastos. Cada auditoría dará origen a un informe de auditoría ("**Informe de auditoría**"), el cual se considerará Información confidencial de MobileIron. El Informe de auditoría expondrá claramente los descubrimientos significativos realizados por el auditor. MobileIron implementará, de buena fe, medidas razonables desde el punto de vista comercial para solucionar (i) los problemas identificados en el Informe de auditoría que puede esperarse razonablemente que afecten la capacidad de MobileIron de cumplir las obligaciones establecidas en la Sección 6 de este DPA y (ii) las deficiencias del control significativas. Si lo solicita el Cliente, MobileIron brindará al Cliente el Informe de auditoría o un resumen elaborado para terceros a fin de que el Cliente pueda verificar si MobileIron cumple con las obligaciones de seguridad establecidas en el DPA. El Informe de auditoría estará sujeto a restricciones de distribución y confidencialidad de MobileIron y del auditor.

b. Revisiones de seguridad. Una vez al año, a menos que la ley disponga lo contrario, y previa notificación presentada en un plazo razonable, MobileIron pondrá a disposición al personal para que el Cliente pueda debatir con este sobre el nivel de cumplimiento de la Sección 6 de este DPA por parte de MobileIron, o bien permitirá que el Cliente acceda a su información o documentación sobre las prácticas de seguridad de la información relacionadas con este DPA, lo que incluye, entre otras cosas, el acceso a informes de evaluación de seguridad elaborados para terceros. Dicha información y documentación deberá considerarse Información confidencial de MobileIron.

13. Términos adicionales para Australia. Esta Sección 13 es válida solo si el Cliente posee usuarios finales en Australia. Los Datos personales se recolectan, almacenan, utilizan o procesan conforme a la Ley de confidencialidad de Australia [Australian Privacy Act] de 1988 (Commonwealth) y a los Principios de confidencialidad de Australia. Si el Cliente no está satisfecho con la forma en que MobileIron maneja una reclamación o no está de acuerdo con la solución propuesta por MobileIron, podrá presentar una reclamación ante la Oficina del Comisionado de Información de Australia (OAIC) y podrá comunicarse con la OAIC a través de los medios mencionados en su sitio web: <https://www.oaic.gov.au/>. Alternativamente, el Cliente podrá solicitar a MobileIron que transfiera los detalles de la reclamación del Cliente directamente a la OAIC.

14. Términos adicionales para Europa. Las Secciones 14 a 19 de este DPA ("**Términos adicionales para Europa**") rigen para el procesamiento de Datos personales de los Usuarios finales del Espacio Económico Europeo ("**EEA**") o Suiza a cargo de MobileIron y en nombre del Cliente. El Artículo 28(1) del Reglamento General de Protección de Datos ("**GDPR**") de la Unión Europea exige la existencia de un contrato entre el controlador y el procesador, y entre el procesador y el subprocesador, además de exigir que el procesamiento se efectúe conforme a las medidas técnicas y organizativas que se ajustan a los requisitos del GDPR y garantizan la protección de los derechos de las personas interesadas. Los Términos adicionales para Europa tienen como objetivo satisfacer dicho requisito en nombre de las partes, siempre y cuando MobileIron actúe como procesador o subprocesador de los Datos personales enviados por el Cliente durante la contratación de Servicios profesionales. En el caso de los términos incluidos en Términos adicionales para Europa y no definidos en esta sección, como "**violación de la seguridad de los datos personales**", "**procesamiento**", "**controlador**", "**procesador**" y "**persona interesada**", se utilizará la definición del Artículo 4 del GDPR.

15. Intención de las partes. Los términos en el Contrato, incluidos los Términos adicionales para Europa y demás disposiciones del DPA, conforman un contrato de procesamiento de datos. En el caso de los Servicios en línea, MobileIron actúa como procesador (o subprocesador) de datos en nombre del Cliente. Como procesador (o subprocesador) de datos, MobileIron solo actuará conforme a las instrucciones del Cliente. El Contrato y el DPA (incluidos los términos y condiciones incorporados por referencia en alguno de ellos), junto con el uso y la configuración de las características de los Servicios en línea por parte del Cliente, componen las instrucciones completas y finales del Cliente para el procesamiento de los Datos de cliente a cargo de MobileIron. Las instrucciones alternativas o adicionales deberán acordarse por escrito.

16. Descripción del procesamiento de datos

a. Objeto y duración. El objeto del procesamiento de los Datos personales es la prestación de los Servicios en línea, incluidos los servicios compatibles. El procesamiento de datos se llevará a cabo durante el Plazo determinado.

- b. **Naturaleza y objetivo.** La naturaleza y el objetivo del procesamiento será prestar Servicios en línea a fin de implementar y brindar las Soluciones de MobileIron y sus características y servicios asociados, brindar soporte al Cliente, ayudar al Cliente a prevenir o solucionar problemas técnicos o de servicio y brindar soporte al Cliente a fin de solucionar los problemas recurrentes e introducir mejoras para el soporte o los Servicios en línea.
- c. **Exportador de datos.** El Cliente actúa como controlador o procesador de los Datos personales y como exportador de datos.
- d. **Importador de datos.** MobileIron, Inc. actúa como procesador o subprocesador de los Datos personales y como importador de datos.
- e. **Personas interesadas.** Las categorías de las Personas interesadas a las que pertenecen los Datos personales son representantes y Usuarios finales del Cliente, en general, personal del Cliente que proporciona los Datos personales a MobileIron a través del uso de la Solución de MobileIron.
- f. **Categorías de datos.** Los tipos de Datos personales procesados, los cuales varían conforme a la Solución de MobileIron y al caso de uso del Cliente, pueden incluir lo siguiente: (i) información de contacto básica de los Usuarios finales para la administración de las cuentas locales y la habilitación de las comunicaciones electrónicas relacionadas con el control de acceso o la gestión de dispositivos móviles; (ii) información básica sobre los dispositivos móviles para su registro, así como para la implementación, la operación y el mantenimiento de las Soluciones de MobileIron; (iii) nombres, direcciones de correo electrónico, nombres de usuario y otros Datos personales del token de autenticación y de los certificados de Inicio de sesión único relacionados con las solicitudes de autenticación de los Usuarios finales y las respuestas a dichas solicitudes para el soporte de la autenticación segura; y (iv) otros datos en formato electrónico utilizados por MobileIron en el contexto de la Solución de MobileIron o enviados por el Cliente durante la contratación de Servicios profesionales.
- g. **Operaciones de procesamiento.** Los Datos personales transferidos estarán sujetos a las siguientes actividades básicas de procesamiento: recolección, almacenamiento, recuperación, consulta, uso, eliminación o destrucción, divulgación por transmisión, difusión o facilitación de los datos del exportador de datos proporcionados a la Solución de MobileIron, según sea necesario, conforme a las instrucciones del exportador de datos, lo que incluye los propósitos internos relacionados (como el control de calidad, la resolución de problemas, el desarrollo del producto, etc.).
- h. **Obligaciones y derechos del Cliente.** Las obligaciones y los derechos del Cliente se establecen en el Contrato y en el DPA.

17. **Transferencia de Datos de cliente y Datos de soporte**

- a. Todas las transferencias de Datos de cliente y Datos de soporte desde el Espacio Económico Europeo y Suiza hacia países que no garantizan un nivel adecuado de protección de datos acorde a las leyes de protección de datos vigentes se registrarán por uno de los siguientes mecanismos de transferencia, en el orden de prioridad especificado: Primero, autocertificaciones para el marco del Escudo de la privacidad UE-EE. UU. y Suiza-EE. UU. de MobileIron para las transferencias hacia los Estados Unidos; segundo, cláusulas modelo para las transferencias de Datos personales a Procesadores en terceros países, las cuales son aprobadas periódicamente por la Comisión Europea; la versión aprobada que se encuentra vigente en la actualidad se incluye en la Decisión 2010/87/EU de la Comisión Europea del 5 de febrero de 2010 y en el Anexo A de los Términos adicionales para Europa (las "**Cláusulas contractuales estándares**"). Las Cláusulas contractuales estándares se rigen por la legislación del Estado miembro donde se haya establecido el Cliente.
- b. MobileIron cumplirá los requisitos establecidos en la ley de protección de datos vigente respecto a la recolección, el uso, la transferencia, la conservación y otros procesamientos de datos personales provenientes del Espacio Económico Europeo y Suiza. MobileIron acuerda notificar al Cliente en caso de determinar que no puede cumplir más con su obligación y brindar el mismo nivel de protección requerido por los principios del Escudo de la privacidad.
- c. La firma de este Contrato por ambas partes incluye la firma de las Cláusulas contractuales estándares. Las Cláusulas contractuales estándares no podrán invocarse para legitimar la exportación de datos desde países en los que se exige una aprobación reglamentaria, a menos que el Cliente haya obtenido dicha aprobación.
- d. En el caso de regir las Cláusulas contractuales estándares, (i) el Cliente aceptará hacer uso de su derecho de auditoría e indicará a MobileIron que realice la auditoría y revisión conforme a lo descrito en la Sección 12, (ii) si el Cliente desea modificar esta indicación, podrá hacerlo conforme a lo establecido en las Cláusulas contractuales estándares y a lo solicitado por escrito y (iii) nada de lo incluido en esta sección generará un cambio o modificación en las Cláusulas contractuales estándares ni generará efecto alguno en los derechos de la autoridad de control o de las personas interesadas conforme a las Cláusulas contractuales estándares.

- 18. **Términos del GDPR.** MobileIron cumplirá con los compromisos establecidos en las Secciones 18 y 19 con entrada en vigencia al inicio de la aplicación del GDPR, del uso de los Servicios en línea por parte del Cliente o de la prestación de Servicios profesionales de MobileIron, lo que ocurra después. La Sección 18 reproduce, con algunas ediciones menores para mayor claridad, los términos contractuales relevantes obligatorios para los procesadores y controladores conforme a los Artículos 28, 32 y 33 del GDPR. Las referencias a los artículos se muestran entre corchetes.

- a. MobileIron no contratará a otro procesador sin la autorización previa, por escrito y específica o general del Cliente. En el caso de la autorización escrita general, MobileIron informará al Cliente los cambios previstos para la adición o el reemplazo de otros procesadores, por lo que el Cliente tendrá la oportunidad de objetar dichos cambios. [28(2)]
- b. MobileIron procesará los Datos personales conforme exclusivamente a las instrucciones documentadas del Cliente, incluidas las instrucciones para transferencias de Datos personales a un tercer país o a una organización internacional, a menos que la legislación de la Unión Europea o del Estado miembro a la que está sujeto MobileIron lo exija; en ese caso, MobileIron informará al Cliente dicho requisito legal antes del procesamiento, a menos que la legislación prohíba dicha información por motivos importantes de interés público. [28(3)]
- c. MobileIron verificará que las personas autorizadas para procesar los Datos personales se hayan comprometido a preservar la confidencialidad de los datos o tengan la obligación legal de preservar la confidencialidad. [28(3)]
- d. MobileIron implementará todas las medidas requeridas en virtud del Artículo 32 del GDPR. [28(3)]
- e. MobileIron respetará las condiciones mencionadas en la Sección 18.a y 18.k respecto a la contratación de otro procesador.
- f. MobileIron tendrá en cuenta la naturaleza del procesamiento y asistirá al Cliente a través de medidas técnicas y organizativas apropiadas, en la medida de lo posible, para que el Cliente pueda cumplir con su obligación y responder las solicitudes de ejercicio de derechos de la persona interesada, los cuales se incluyen en el Capítulo III del GDPR. [28(3)]
- g. MobileIron asistirá al Cliente para garantizar el cumplimiento de las obligaciones conforme a los Artículos 32 a 36 del GDPR, teniendo en cuenta la naturaleza del procesamiento y la información disponible para MobileIron. [28(3)]
- h. MobileIron podrá, a elección del Cliente, eliminar o devolver todos los Datos personales al Cliente tras finalizar la prestación de servicios relacionados con el procesamiento, así como eliminar las copias existentes, a menos que la legislación de la Unión Europea o del Estado miembro exija el almacenamiento de los Datos personales. [28(3)]
- i. MobileIron pondrá a disposición del Cliente toda la información necesaria para demostrar el cumplimiento de las obligaciones expuestas en el Artículo 28 del GDPR y facilitará y colaborará con las auditorías, incluidas las inspecciones, realizadas por el Cliente o por un auditor designado por el Cliente. [28(3)]
- j. MobileIron informará de inmediato al Cliente si, en su opinión, una instrucción infringe el GDPR u otras disposiciones de la Unión Europea o del Estado miembro respecto a la protección de datos. [28(3)]
- k. Si MobileIron contrata a otro procesador para el desarrollo de actividades específicas de procesamiento en nombre del Cliente, se impondrán al procesador las mismas obligaciones de protección de datos del Artículo 28(3) del GDPR (las cuales se reproducen en la Sección 18.b-19.j) a través de un contrato u otro instrumento jurídico conforme a la legislación de la Unión Europea o del Estado miembro, lo que garantizará, en particular, la implementación de medidas técnicas y organizativas apropiadas, por lo que el procesamiento podrá cumplir con los requisitos del GDPR. Si el otro procesador no cumple con las obligaciones relacionadas con la protección de datos, MobileIron será plenamente responsable ante el Cliente del cumplimiento de las obligaciones del otro procesador. [28(4)]
- l. Teniendo en cuenta el panorama actual, los costos de implementación y la naturaleza, el alcance, el contexto y el propósito del procesamiento, así como el riesgo de que existan diversas probabilidades y grados variables de derechos y libertades de las personas físicas, el Cliente y MobileIron deberán implementar medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad apropiado ante dicho riesgo, lo que incluye, entre otras cosas y según corresponda, las siguientes: (i) la seudonimización y encriptación de los Datos personales; (ii) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y adaptación continuas de los sistemas y servicios de procesamiento; (iii) la capacidad de restaurar la disponibilidad y el acceso a los Datos personales de manera oportuna en caso de que surja un incidente físico o técnico; y (iv) un proceso para evaluar, examinar y analizar regularmente la eficacia de las medidas técnicas y organizativas a fin de garantizar la seguridad del procesamiento. [32(1)]
- m. Al evaluar el nivel apropiado de seguridad, se deben tener en cuenta los riesgos generados por el procesamiento, específicamente los causados por la destrucción, la pérdida, la alteración, la divulgación no autorizada o el acceso, ya sean ilegales o accidentales, a los Datos personales transmitidos, almacenados o procesados. [32(2)]
- n. El Cliente y MobileIron deberán implementar medidas para garantizar que la persona física que actúe bajo la autoridad del Cliente o MobileIron y que acceda a los Datos personales no procese dichos datos de una manera no indicada en las instrucciones del Cliente, a menos la legislación de la Unión Europea o del Estado miembro lo exija. [32(4)]
- o. MobileIron notificará al Cliente sin demoras indebidas luego de tomar conocimiento sobre la violación de la seguridad de los datos personales. [33(2)] Dicha notificación debe, como mínimo, (i) describir la naturaleza de la violación de la seguridad de los datos personales e incluir, en lo posible, las categorías y la cantidad aproximada de personas interesadas afectadas, así como las categorías y cantidad aproximada de registros de Datos personales afectados; (ii) comunicar el nombre y los detalles de contacto del oficial de protección de datos o de otro contacto que posea más información; (iii) describir las posibles consecuencias que puede generar la violación de la seguridad de los datos personales; y (iv) describir las medidas implementadas o propuestas por el controlador para solucionar la violación de la seguridad de los datos personales, lo que incluye, si corresponde, medidas para mitigar los posibles efectos adversos. [33(3)]

19. **Términos adicionales del GDPR.** Esta Sección 19 proporciona más detalles sobre lo que el Cliente puede esperar de MobileIron respecto al cumplimiento de los términos de la Sección 18, así como los compromisos que asume MobileIron respecto a los Artículos 34-36 del GDPR que no se incluyen en otros puntos del Contrato.

a. **Subprocesadores.** El Cliente autoriza a MobileIron a contratar a Subprocesadores para que procesen los Datos personales conforme a la Sección 18.a y 18.k. La lista de Subprocesadores actuales de MobileIron se encuentra disponible bajo solicitud o en el sitio web de MobileIron. MobileIron actualizará la lista al menos 14 días antes de permitir que un Subprocesador nuevo acceda a los Datos personales. En el caso de que MobileIron actúe como procesador (y no subprocesador), se aplicarán los siguientes términos: (i) Si el Cliente no aprueba a un Subprocesador nuevo, el Cliente podrá cancelar la suscripción de los Servicios en línea afectados sin sufrir ninguna penalización; para esto, deberá presentar, antes de que finalice el período de notificación, una notificación de cancelación por escrito que incluya los motivos por los que no se aprobó al Subprocesador; (ii) si los Servicios en línea afectados forman parte de un paquete (o de una compra individual similar de varios servicios), la cancelación se aplicará a todo el paquete; y (iii) como reparación única y exclusiva para el Cliente, MobileIron reembolsará al Cliente las tarifas de suscripción prepagadas y no utilizadas.

b. **Solicitudes de Personas interesadas.** MobileIron pondrá a disposición del Cliente los Datos personales de las personas interesadas y permitirá que satisfaga las solicitudes de las personas interesadas para ejercer uno o más de sus derechos conforme al GDPR, de una manera que sea consecuente con la funcionalidad de los Servicios en línea y la función de MobileIron como procesador. Si el Cliente no puede responder a una solicitud de una persona interesada mediante la funcionalidad de los Servicios en línea, MobileIron responderá las solicitudes de asistencia razonables del Cliente para que pueda brindar dichas respuestas. Si MobileIron recibe una solicitud de una persona interesada del Cliente para ejercer uno o más de sus derechos conforme al GDPR, MobileIron redirigirá a la persona interesada para que presente la solicitud directamente al Cliente.

c. **Revisiones de seguridad, auditorías e inspecciones.** El Informe de auditoría y demás documentación e información descrita en la Sección 12 tiene como objetivo proporcionar evidencia sobre el cumplimiento, por parte de MobileIron, de las medidas técnicas y organizativas que contribuyen a la protección de los Servicios en línea conforme a los objetivos establecidos en la Sección 18.i. MobileIron pondrá a disposición del Cliente, previa solicitud escrita, un resumen de los términos del procesamiento de datos incluidos en los contratos con los Subprocesadores. El Cliente podrá solicitar por escrito información adicional razonable respecto a la capacidad del Subprocesador para desarrollar las actividades de procesamiento relevantes de acuerdo con este DPA.

d. **Evaluaciones sobre el impacto en la protección de datos.** MobileIron brindará al Cliente, previa solicitud, la información razonable que este último necesita para cumplir con las evaluaciones sobre el impacto en la protección de datos, si hubiera, conforme a la obligación mencionada en la Sección 18.g.

20. **Asistencia.** El Cliente deberá presentar una solicitud por escrito para recibir la asistencia mencionada en este DPA. MobileIron podrá cobrar al Cliente un cargo razonable por dicha asistencia, el cual se incluirá en un presupuesto y se acordará entre las partes.

MOBILEIRON, INC.
Términos adicionales para Europa
Anexo A: Cláusulas contractuales estándares (Procesadores)
(versión del 15 de mayo de 2018)

A efectos del artículo 26, apartado 2, de la Directiva 95/46/CE para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países que no garanticen una adecuada protección de los datos.

Cliente

(el “exportador de datos”)

y

MobileIron, Inc.

401 East Middlefield Road, Mountain View, CA 94043, USA (el “importador de datos”)

cada uno de ellos, una “parte”; en conjunto, “las partes”,

cada una de ellas «la parte»; conjuntamente «las partes»

ACUERDAN las siguientes cláusulas contractuales (en lo sucesivo, las «cláusulas») con objeto de ofrecer garantías suficientes respecto de la protección de la vida privada y los derechos y libertades fundamentales de las personas para la transferencia por el exportador de datos al importador de datos de los datos personales especificados en el apéndice 1.

Cláusula 1
Definiciones

A los efectos de las presentes cláusulas:

- a) «datos personales», «categorías especiales de datos», «tratamiento», «responsable del tratamiento», «encargado del tratamiento», «interesado» y «autoridad de control» tendrán el mismo significado que en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos¹;
- b) por «exportador de datos» se entenderá el responsable del tratamiento que transfiera los datos personales;
- c) por «importador de datos» se entenderá el encargado del tratamiento que convenga en recibir del exportador datos personales para su posterior tratamiento en nombre de este, de conformidad con sus instrucciones y de los términos de las cláusulas, y que no esté sujeto al sistema de un tercer país por el que se garantice la protección adecuada en el sentido del artículo 25, apartado 1, de la Directiva 95/46/CE;
- d) por «subencargado del tratamiento» se entenderá cualquier encargado del tratamiento contratado por el importador de datos o por cualquier otro subencargado de este que convenga en recibir del importador de datos, o de cualquier otro subencargado de este, datos personales exclusivamente para las posteriores actividades de tratamiento que se hayan de llevar a cabo en nombre del exportador de datos, de conformidad con sus instrucciones, los términos de las cláusulas y los términos del contrato que se haya concluido por escrito;
- e) por «legislación de protección de datos aplicable» se entenderá la legislación que protege los derechos y libertades fundamentales de las personas y, en particular, su derecho a la vida privada respecto del tratamiento de los datos personales, aplicable al responsable del tratamiento en el Estado miembro en que está establecido el exportador de datos;
- f) por «medidas de seguridad técnicas y organizativas» se entenderán las destinadas a proteger los datos personales contra su destrucción accidental o ilícita o su pérdida accidental, su alteración, divulgación o acceso no autorizados, especialmente cuando el tratamiento suponga la transmisión de los datos por redes, o cualquier otra forma ilícita de tratamiento.

Cláusula 2
Detalles de la transferencia

Los detalles de la transferencia, en particular, las categorías especiales de los datos personales, quedan especificados si procede en el apéndice 1, que forma parte integrante de las presentes cláusulas.

¹ Las partes podrán reproducir en esta cláusula las definiciones y significados de la Directiva 95/46/CE si consideran que ello beneficia a la autonomía del contrato.

Cláusula 3
Cláusula de tercero beneficiario

1. Los interesados podrán exigir al exportador de datos el cumplimiento de la presente cláusula, las letras b) a i) de la cláusula 4, las letras a) a e) y g) a j) de la cláusula 5, los apartados 1 y 2 de la cláusula 6, la cláusula 7, el apartado 2 de la cláusula 8 y las cláusulas 9 a 12, como terceros beneficiarios.
2. Los interesados podrán exigir al importador de datos el cumplimiento de la presente cláusula, las letras a) a e) y g) de la cláusula 5, la cláusula 6, la cláusula 7, el apartado 2 de la cláusula 8 y las cláusulas 9 a 12, cuando el exportador de datos haya desaparecido de facto o haya cesado de existir jurídicamente, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos en virtud de contrato o por ministerio de la ley y a resultas de lo cual asuma los derechos y las obligaciones del exportador de datos, en cuyo caso los interesados podrán exigirlos a dicha entidad.
3. Los interesados podrán exigir al subencargado del tratamiento de datos el cumplimiento de la presente cláusula, las letras a) a e) y g) de la cláusula 5, la cláusula 6, la cláusula 7, el apartado 2 de la cláusula 8 y las cláusulas 9 a 12, en aquellos casos en que ambos, el exportador de datos y el importador de datos, hayan desaparecido de facto o hayan cesado de existir jurídicamente o sean insolventes, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos en virtud de contrato o por ministerio de la ley, a resultas de lo cual asuma los derechos y las obligaciones del exportador de datos, en cuyo caso los interesados podrán exigirlos a dicha entidad. Dicha responsabilidad civil del subencargado del tratamiento de datos se limitará a sus propias operaciones de tratamiento de datos con arreglo a las cláusulas.
4. Las partes no se oponen a que los interesados estén representados por una asociación u otras entidades, si así lo desean expresamente y lo permite el Derecho nacional.

Cláusula 4
Obligaciones del exportador de datos

El exportador de datos acuerda y garantiza lo siguiente:

- a) el tratamiento de los datos personales, incluida la propia transferencia, ha sido efectuado y seguirá efectuándose de conformidad con las normas pertinentes de la legislación de protección de datos aplicable (y, si procede, se ha notificado a las autoridades correspondientes del Estado miembro de establecimiento del exportador de datos) y no infringe las disposiciones legales o reglamentarias en vigor en dicho Estado miembro;
- b) ha dado al importador de datos, y dará durante la prestación de los servicios de tratamiento de los datos personales, instrucciones para que el tratamiento de los datos personales transferidos se lleve a cabo exclusivamente en nombre del exportador de datos y de conformidad con la legislación de protección de datos aplicable y con las cláusulas;
- c) el importador de datos ofrecerá garantías suficientes en lo que respecta a las medidas de seguridad técnicas y organizativas especificadas en el apéndice 2 del presente contrato;
- d) ha verificado que, de conformidad con la legislación de protección de datos aplicable, dichas medidas resultan apropiadas para proteger los datos personales contra su destrucción accidental o ilícita o su pérdida accidental, su alteración, divulgación o acceso no autorizados, especialmente cuando el tratamiento suponga la transmisión de los datos por redes, o contra cualquier otra forma ilícita de tratamiento y que dichas medidas garantizan un nivel de seguridad apropiado a los riesgos que entraña el tratamiento y la naturaleza de los datos que han de protegerse, habida cuenta del estado de la técnica y del coste de su aplicación;
- e) asegurará que dichas medidas se lleven a la práctica;
- f) si la transferencia incluye categorías especiales de datos, se habrá informado a los interesados, o serán informados antes de que se efectúe aquella, o en cuanto sea posible, de que sus datos podrían ser transferidos a un tercer país que no proporciona la protección adecuada en el sentido de la Directiva 95/46/CE;
- g) enviará la notificación recibida del importador de datos o de cualquier subencargado del tratamiento de datos a la autoridad de control de la protección de datos, de conformidad con la letra b) de la cláusula 5 y el apartado 3 de la cláusula 8, en caso de que decida proseguir la transferencia o levantar la suspensión;
- h) pondrá a disposición de los interesados, previa petición de estos, una copia de las cláusulas, a excepción del apéndice 2, y una descripción sumaria de las medidas de seguridad, así como una copia de cualquier contrato para los servicios de subtratamiento de los datos que debe efectuarse de conformidad con las cláusulas, a menos que las cláusulas o el contrato contengan información comercial, en cuyo caso podrá eliminar dicha información comercial;

- i) que, en caso de subtratamiento, la actividad de tratamiento se llevará a cabo de conformidad con la cláusula 11 por un subencargado del tratamiento que proporcionará por lo menos el mismo nivel de protección de los datos personales y los derechos de los interesados que el importador de datos en virtud de las presentes cláusulas; y
- j) que asegurará que las letras a) a i) de la cláusula 4 se lleven a la práctica.

Cláusula 5
Obligaciones del importador de datos²

El importador de datos acuerda y garantiza lo siguiente:

- a) tratará los datos personales transferidos solo en nombre del exportador de datos, de conformidad con sus instrucciones y las cláusulas. En caso de que no pueda cumplir estos requisitos por la razón que fuere, informará de ello sin demora al exportador de datos, en cuyo caso este estará facultado para suspender la transferencia de los datos o rescindir el contrato;
- b) no tiene motivos para creer que la legislación que le es de aplicación le impida cumplir las instrucciones del exportador de datos y sus obligaciones a tenor del contrato y que, en caso de modificación de la legislación que pueda tener un impotente efecto negativo sobre las garantías y obligaciones estipuladas en las cláusulas, notificará al exportador de datos dicho cambio en cuanto tenga conocimiento de él, en cuyo caso este estará facultado para suspender la transferencia de los datos o rescindir el contrato;
- c) ha puesto en práctica las medidas de seguridad técnicas y organizativas que se indican en el apéndice 2 antes de efectuar el tratamiento de los datos personales transferidos;
- d) notificará sin demora al exportador de datos sobre:
 - i) toda solicitud jurídicamente vinculante de divulgar los datos personales presentada por una autoridad encargada de la aplicación de ley a menos que esté prohibido, por ejemplo, por el Derecho penal para preservar la confidencialidad de una investigación llevada a cabo por una de dichas autoridades,
 - ii) todo acceso accidental o no autorizado,
 - iii) toda solicitud sin respuesta recibida directamente de los interesados, a menos que se le autorice;
- e) tratará adecuadamente en los períodos de tiempo prescritos todas las consultas del exportador de datos relacionadas con el tratamiento que este realice de los datos personales sujetos a transferencia y se atenderá a la opinión de la autoridad de control en lo que respecta al tratamiento de los datos transferidos;
- f) ofrecerá a petición del exportador de datos sus instalaciones de tratamiento de datos para que se lleve a cabo la auditoría de las actividades de tratamiento cubiertas por las cláusulas. Esta será realizada por el exportador de datos o por un organismo de inspección, compuesto por miembros independientes con las cualificaciones profesionales necesarias y sujetos a la confidencialidad, seleccionado por el exportador de datos y, cuando corresponda, de conformidad con la autoridad de control;
- g) pondrá a disposición de los interesados, previa petición de estos, una copia de las cláusulas, o de cualquier contrato existente para el subtratamiento de los datos, a menos que las cláusulas o el contrato contengan información comercial, en cuyo caso podrá eliminar dicha información comercial, a excepción del apéndice 2 que será sustituido por una descripción sumaria de las medidas de seguridad, en aquellos casos en que el interesado no pueda obtenerlas directamente del exportador de datos;
- h) que, en caso de subtratamiento de los datos, habrá informado previamente al exportador de datos y obtenido previamente su consentimiento por escrito;
- i) que los servicios de tratamiento por el subencargado del tratamiento se llevarán a cabo de conformidad con la cláusula 11;
- j) enviará sin demora al exportador de datos una copia de cualquier acuerdo con el subencargado del tratamiento que concluya con arreglo a las cláusulas.

² Las obligaciones impuestas por la legislación nacional aplicable al importador de datos que no vayan más allá de las restricciones necesarias en una sociedad democrática con arreglo a los intereses recogidos en el artículo 13, apartado 1, de la Directiva 95/46/CE, es decir, si dichas obligaciones constituyen una medida necesaria para la salvaguardia de la seguridad del Estado; la defensa; la seguridad pública; la prevención, investigación, detección y enjuiciamiento de delitos o infracciones de la deontología en las profesiones reguladas; un interés económico o financiero importante del Estado o la protección del interesado o de los derechos y libertades de otras personas, no están en contradicción con las cláusulas contractuales tipo. Algunos ejemplos de obligaciones que no van más allá de las restricciones necesarias en una sociedad democrática son, entre otras, las sanciones reconocidas en el ámbito internacional, las obligaciones de notificación en materia fiscal o las impuestas por la lucha contra el blanqueo de dinero.

Cláusula 6
Responsabilidad

1. Las partes acuerdan que los interesados que hayan sufrido daños como resultado del incumplimiento de las obligaciones mencionadas en la cláusula 3 o en la cláusula 11 por cualquier parte o subencargado del tratamiento tendrán derecho a percibir una indemnización del exportador de datos para el daño sufrido.
2. En caso de que el interesado no pueda interponer contra el exportador de datos la demanda de indemnización a que se refiere el apartado 1 por incumplimiento por parte del importador de datos o su subencargado de sus obligaciones impuestas en la cláusulas 3 o en la cláusula 11, por haber desaparecido de facto, cesado de existir jurídicamente o ser insolvente, el importador de datos acepta que el interesado pueda demandarle a él en el lugar del exportador de datos, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos en virtud de contrato o por ministerio de la ley, en cuyo caso los interesados podrán exigir sus derechos a dicha entidad.

El importador de datos no podrá basarse en un incumplimiento de un subencargado del tratamiento de sus obligaciones para eludir sus propias responsabilidades.

3. En caso de que el interesado no pueda interponer contra el exportador de datos o el importador de datos la demanda a que se refieren los apartados 1 y 2, por incumplimiento por parte del subencargado del tratamiento de datos de sus obligaciones impuestas en la cláusula 3 o en la cláusula 11, por haber desaparecido de facto, cesado de existir jurídicamente o ser insolventes ambos, tanto el exportador de datos como el importador de datos, el subencargado del tratamiento de datos acepta que el interesado pueda demandarle a él en cuanto a sus propias operaciones de tratamiento de datos en virtud de las cláusulas en el lugar del exportador de datos o del importador de datos, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos o del importador de datos en virtud de contrato o por ministerio de la ley, en cuyo caso los interesados podrán exigir sus derechos a dicha entidad. La responsabilidad del subencargado del tratamiento se limitará a sus propias operaciones de tratamiento de datos con arreglo a las presentes cláusulas.

Cláusula 7
Mediación y jurisdicción

1. El importador de datos acuerda que, si el interesado invoca en su contra derechos de tercero beneficiario o reclama una indemnización por daños y perjuicios con arreglo a las cláusulas, aceptará la decisión del interesado de:
 - a) someter el conflicto a mediación por parte de una persona independiente o, si procede, por parte de la autoridad de control;
 - b) someter el conflicto a los tribunales del Estado miembro de establecimiento del exportador de datos.
2. Las partes acuerdan que las opciones del interesado no obstaculizarán sus derechos sustantivos o procedimentales a obtener reparación de conformidad con otras disposiciones de Derecho nacional o internacional.

Cláusula 8
Cooperación con las autoridades de control

1. El exportador de datos acuerda depositar una copia del presente contrato ante la autoridad de control si así lo requiere o si el depósito es exigido por la legislación de protección de datos aplicable.
2. Las partes acuerdan que la autoridad de control está facultada para auditar al importador, o a cualquier subencargado, en la misma medida y condiciones en que lo haría respecto del exportador de datos conforme a la legislación de protección de datos aplicable.
3. El importador de datos informará sin demora al exportador de datos en el caso de que la legislación existente aplicable a él o a cualquier subencargado no permita auditar al importador ni a los subencargados, con arreglo al apartado 2. En tal caso, el importador de datos estará autorizado a adoptar las medidas previstas en la letra b) de la cláusula 5.

Cláusula 9
Legislación aplicable

Las cláusulas se regirán por la legislación del Estado miembro de establecimiento del exportador de datos.

Cláusula 10
Variación del contrato

Las partes se comprometen a no variar o modificar las presentes cláusulas. Esto no excluye que las partes añadan cláusulas relacionadas con sus negocios en caso necesario siempre que no contradigan las cláusulas.

Cláusula 11
Subtratamiento de datos

1. El importador de datos no subcontratará ninguna de sus operaciones de procesamiento llevadas a cabo en nombre del exportador de datos con arreglo a las cláusulas sin previo consentimiento por escrito del exportador de datos. Si el importador de datos subcontrata sus obligaciones con arreglo a las cláusulas, con el consentimiento del exportador de datos, lo hará exclusivamente mediante un acuerdo escrito con el subencargado del tratamiento de datos, en el que se le impongan a este las mismas obligaciones impuestas al importador de datos con arreglo a las cláusulas.³ En los casos en que el subencargado del tratamiento de datos no pueda cumplir sus obligaciones de protección de los datos con arreglo a dicho acuerdo escrito, el importador de datos seguirá siendo plenamente responsable frente al exportador de datos del cumplimiento de las obligaciones del subencargado del tratamiento de datos con arreglo a dicho acuerdo.
2. El contrato escrito previo entre el importador de datos y el subencargado del tratamiento contendrá asimismo una cláusula de tercero beneficiario, tal como se establece en la cláusula 3, para los casos en que el interesado no pueda interponer la demanda de indemnización a que se refiere el apartado 1 de la cláusula 6 contra el exportador de datos o el importador de datos por haber estos desaparecido de facto, cesado de existir jurídicamente o ser insolventes, y ninguna entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos o del importador de datos en virtud de contrato o por ministerio de la ley. Dicha responsabilidad civil del subencargado del tratamiento se limitará a sus propias operaciones de tratamiento de datos con arreglo a las cláusulas
3. Las disposiciones sobre aspectos de la protección de los datos en caso de subcontratación de operaciones de procesamiento a que se refiere el apartado 1 se regirán por la legislación del Estado miembro de establecimiento del exportador de datos.
4. El exportador de datos conservará la lista de los acuerdos de subtratamiento celebrados con arreglo a las cláusulas y notificados por el importador de datos de conformidad con la letra j) de la cláusula 5, lista que se actualizará al menos una vez al año. La lista estará a disposición de la autoridad de control de protección de datos del exportador de datos.

Cláusula 12
Obligaciones una vez finalizada la prestación de los servicios de tratamiento de los datos personales

1. Las partes acuerdan que, una vez finalizada la prestación de los servicios de tratamiento de los datos personales, el importador y el subencargado deberán, a discreción del exportador, o bien devolver todos los datos personales transferidos y sus copias, o bien destruirlos por completo y certificar esta circunstancia al exportador, a menos que la legislación aplicable al importador le impida devolver o destruir total o parcialmente los datos personales transferidos. En tal caso, el importador de datos garantiza que guardará el secreto de los datos personales transferidos y que no volverá a someterlos a tratamiento.
2. El importador de datos y el subencargado garantizan que, a petición del exportador o de la autoridad de control, pondrá a disposición sus instalaciones de tratamiento de los datos para que se lleve a cabo la auditoría de las medidas mencionadas en el apartado 1.

APÉNDICE 1 A LAS CLÁUSULAS CONTRACTUALES TIPO

El presente apéndice forma parte integrante de las cláusulas y deberá ser cumplimentado y suscrito por las partes.

Exportador de datos: El Cliente actúa como exportador de datos.

Importador de datos: MobileIron, Inc. actúa como importador de datos.

Interesados: Consulte la Sección 16 del DPA.

Categorías de datos: Consulte la Sección 16 del DPA.

Categorías especiales de datos (si es pertinente): Consulte la Sección 16 del DPA.

Operaciones de tratamiento: Consulte la Sección 16 del DPA.

³ Este requisito puede verse satisfecho si el subencargado es cosignatario del contrato acordado entre el exportador de datos y el importador de datos con arreglo a la presente Decisión.

APÉNDICE 2 A LAS CLÁUSULAS CONTRACTUALES TIPO

El presente Apéndice forma parte integrante de las cláusulas y deberá ser cumplimentado y suscrito por las partes.

Descripción de las medidas de seguridad técnicas y organizativas puestas en práctica por el importador de datos de conformidad con la letra d) de la cláusula 4 y la letra c) de la cláusula 5 (o documento o legislación adjuntos): Conforme a lo descrito en la Sección 6 del DPA.