

Contrato de Encargo de Tratamiento

DeskTime · SIA DeskTime — Riga, Letonia

El presente contrato de encargo de tratamiento de datos personales («**DPA**») forma parte integrante de las Condiciones de Servicio para el uso de DeskTime y constituye un acuerdo vinculante entre SIA DeskTime («**DeskTime**») y cualquier persona física o jurídica («**Ciente**») que utilice el servicio de seguimiento del tiempo de DeskTime y cualquier otro Servicio prestado por DeskTime («**Servicio**»), distinto del uso personal y privado, para supervisar y tratar datos personales de sus empleados u otras personas («**Interesados**» o «**Usuarios Finales**») dentro de su cuenta de DeskTime.

1. Definiciones

- «**Leyes de Protección de Datos**» significa el RGPD y las leyes que lo desarrollen o complementen, en la medida en que resulten aplicables;
- «**RGPD**» significa el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE;
- «**Violación de Datos Personales**» significa una violación de la seguridad que provoque la destrucción, pérdida o alteración accidental o ilícita, o la comunicación o el acceso no autorizados, a Datos Personales transmitidos, conservados o tratados de otra forma (en cada caso, según se define en el RGPD);
- «**Datos Personales**» significa cualquier información relativa a un interesado (según se define en las Leyes de Protección de Datos);
- «**Cláusulas Contractuales Tipo**» significa las cláusulas contractuales tipo para las transferencias de datos entre la UE y países no pertenecientes a la UE, adoptadas por la Comisión Europea, según sean modificadas cuando corresponda;
- «**Subencargado**» significa cualquier entidad (incluido cualquier tercero, pero excluyendo a los empleados de DeskTime) contratada por DeskTime para tratar Datos Personales por cuenta del Cliente;
- «**Terceros Países**» significa todos los países situados fuera del Espacio Económico Europeo, excluyendo aquellos países que la Comisión Europea considere que ofrecen una protección adecuada de los Datos Personales;
- Los términos «controlador», «datos personales», «tratamiento», «encargado del tratamiento» y «autoridad de control» tendrán el mismo significado que en el RGPD y sus términos derivados se interpretarán en consecuencia;
- Salvo que se defina de otro modo en el presente documento, todos los términos en mayúsculas utilizados en este DPA tendrán el significado que se les atribuye en las Condiciones de Servicio. En caso de conflicto entre las definiciones de este DPA y las de las Condiciones de Servicio, prevalecerán las definiciones de este DPA únicamente a efectos de las actividades de tratamiento de datos reguladas por el mismo.

2. Ámbito y funciones

2.1 Este DPA se aplica al tratamiento de Datos Personales en el ámbito del Servicio prestado por DeskTime a los Clientes en relación con los servicios de seguimiento del tiempo y cualquier otro Servicio prestado por DeskTime. Este DPA constituye un anexo a las Condiciones de Servicio, que regulan los derechos y obligaciones de las partes en relación con el Servicio prestado por DeskTime.

2.2 A efectos del tratamiento de Datos Personales en virtud de este DPA, el Cliente tendrá la consideración de responsable del tratamiento, y DeskTime tendrá la consideración de encargado del tratamiento.

3. Detalles del tratamiento

3.1 DeskTime tratará los Datos Personales de manera coherente con este DPA, con las instrucciones del Cliente y/o en la medida necesaria para prestar los Servicios al Cliente conforme a las Condiciones de Servicio, según se detalla además en el Anexo 1. Para evitar dudas, salvo acuerdo por escrito entre las Partes, DeskTime no estará autorizada a tratar los Datos Personales para sus propios fines.

3.2 Las Partes se comprometen a cumplir con sus obligaciones conforme a las Leyes de Protección de Datos. Cada Parte es la única responsable del cumplimiento de las Leyes de Protección de Datos que le resulten aplicables.

3.3 Si DeskTime no puede cumplir las instrucciones del Cliente por cualquier motivo (incluido el caso de que la instrucción vulnere las Leyes de Protección de Datos), se compromete a informar al Cliente de su incapacidad para cumplirlas tan pronto como sea razonablemente posible. La falta de notificación por parte de DeskTime no afectará a la responsabilidad del Cliente por sus instrucciones.

3.4 El Cliente confirma que este DPA, junto con la configuración o el uso por parte del Cliente de cualquier ajuste, función u opción del Servicio (que el Cliente pueda modificar en cualquier momento), constituye una instrucción suficiente a DeskTime en relación con el tratamiento de Datos Personales y que, por tanto, constituye un acuerdo de tratamiento de datos vinculante conforme a las Leyes de Protección de Datos.

4. Obligaciones del Cliente

4.1 El Cliente declara y garantiza que ha cumplido y seguirá cumpliendo con toda la legislación aplicable, incluidas las Leyes de Protección de Datos, en relación con el tratamiento de los Datos Personales de los Usuarios Finales y con cualquier instrucción de tratamiento que dé a DeskTime.

4.2 El Cliente declara y garantiza que los Datos Personales de los Usuarios Finales se han recopilado sobre una base válida y lícita, que ha proporcionado todos los avisos exigidos y ha obtenido todos los consentimientos, permisos y derechos necesarios conforme a las Leyes de Protección de Datos, y que está facultado para transferir o poner de otro modo a disposición de DeskTime dichos Datos Personales de los Usuarios Finales para su tratamiento conforme a los fines descritos en este DPA. El Cliente será el único responsable de la exactitud, calidad, licitud y forma de obtención de los Datos Personales de los Usuarios Finales.

5. Devolución o supresión de los Datos Personales

5.1 DeskTime tratará los Datos Personales mientras el Cliente disponga de una cuenta en DeskTime. El Cliente podrá, en cualquier momento, solicitar la supresión de los Datos Personales de los Usuarios Finales y exportar dichos datos utilizando las funcionalidades disponibles en los Servicios.

5.2 Al finalizar o expirar las Condiciones de Servicio, DeskTime, a elección del Cliente, suprimirá o devolverá los Datos Personales de los Usuarios Finales (incluso permitiendo la exportación de datos mediante las funcionalidades disponibles) y eliminará cualquier copia restante, salvo que la legislación aplicable exija su conservación. DeskTime podrá aplicar una anonimización irreversible en lugar de la supresión cuando resulte procedente. A petición del Cliente, DeskTime confirmará por escrito dicha supresión o devolución.

5.3 Salvo que la legislación aplicable exija o permita lo contrario, DeskTime no tendrá obligación de conservar los datos del Cliente tras la finalización del acuerdo de Servicio con el Cliente.

6. Subencargados

6.1 DeskTime trabaja con terceros (Subencargados) que prestan a DeskTime distintos servicios necesarios en el curso ordinario de su actividad. Los subencargados actualmente contratados por DeskTime y autorizados por el Cliente están disponibles [aquí](#).

6.2 DeskTime podrá seguir utilizando los Subencargados ya contratados en la fecha de este DPA, garantizando que:

- 6.2.1 DeskTime ha llevado a cabo una diligencia debida adecuada para garantizar que el Subencargado es capaz de ofrecer un nivel de protección suficiente para los Datos Personales;
- 6.2.2 DeskTime se ha asegurado de que el acuerdo entre DeskTime y el Subencargado correspondiente esté regulado por un contrato escrito que incluya condiciones que ofrezcan, como mínimo, el mismo nivel de protección de los Datos Personales que las establecidas en este DPA y que cumplan los requisitos del artículo 28, apartado 3, del RGPD.

6.3 Si alguno de los Subencargados contratados no puede cumplir con sus obligaciones conforme al acuerdo de tratamiento de datos mencionado en la Sección 6.2.2, DeskTime seguirá siendo plenamente responsable ante el Cliente de las obligaciones y actividades del Subencargado. DeskTime será responsable de cualquier consecuencia derivada de las actividades del Subencargado en relación con el tratamiento de Datos Personales.

6.4 DeskTime notificará al Cliente con 30 días de antelación cualquier cambio previsto en los Subencargados. Si el Cliente se opone al Subencargado propuesto por motivos razonables de protección de datos, deberá notificarlo por escrito a DeskTime en un plazo de 15 días, especificando el motivo de la objeción. DeskTime considerará dicha objeción de buena fe y podrá, a su discreción, adoptar medidas razonables para atender la inquietud. Si la objeción no puede resolverse razonablemente, DeskTime podrá abstenerse de contratar al Subencargado para el tratamiento en cuestión o permitir que

el Cliente ponga fin al uso de los Servicios. En tales casos, el Cliente no será responsable, conforme a las Condiciones de Servicio ni a la legislación aplicable, por dicha terminación.

6.5 Con sujeción a los requisitos de la Cláusula 6.2, el Cliente acepta que DeskTime pueda utilizar Subencargados situados fuera del Espacio Económico Europeo (EEE). En tales casos, DeskTime garantizará que cualquier transferencia y tratamiento de Datos Personales cumpla con las Leyes de Protección de Datos aplicables, incluso mediante el uso de las Cláusulas Contractuales Tipo de la UE, decisiones de adecuación de la Comisión Europea u otros mecanismos de transferencia válidos reconocidos por la legislación aplicable.

7. Seguridad

7.1 DeskTime adoptará las medidas técnicas, organizativas y administrativas adecuadas destinadas a proteger la confidencialidad, integridad y disponibilidad de los Datos Personales. Las medidas de seguridad específicas aplicadas por DeskTime se describen en el Anexo 1 de este DPA.

7.2 DeskTime tratará todos los Datos Personales como confidenciales. DeskTime se asegurará de que todas las personas y partes (empleados, agentes y demás personas implicadas en el tratamiento de los Datos Personales) hayan firmado y estén sujetas a un acuerdo de confidencialidad adecuado o a cualquier otra obligación vinculante de confidencialidad.

7.3 DeskTime no incumplirá la obligación de no divulgación si la divulgación de datos personales es obligatoria conforme a la legislación aplicable.

8. Violación de Datos Personales

8.1 En caso de Violación de Datos Personales, DeskTime notificará al Cliente sin dilación indebida y de conformidad con las obligaciones establecidas en las Leyes de Protección de Datos. Al notificar al Cliente, DeskTime proporcionará información sobre la naturaleza de la Violación de Datos Personales, sus posibles consecuencias, un punto de contacto para obtener más información y las medidas adoptadas o propuestas para abordar y mitigar la violación.

8.2 Si la información no puede facilitarse de forma simultánea, podrá proporcionarse por fases y sin dilación indebida.

8.3 Ninguna notificación o respuesta de DeskTime en relación con una Violación de Datos Personales se interpretará como una admisión de culpa o responsabilidad. DeskTime no será responsable de revisar ni determinar las obligaciones legales o normativas de notificación aplicables al Cliente. El Cliente seguirá siendo el único responsable de evaluar y cumplir cualquier obligación de notificar a las autoridades reguladoras o a los interesados en caso de una Violación de Datos Personales.

8.4 Las notificaciones de Violación de Datos Personales se enviarán al punto de contacto principal del Cliente establecido en la cuenta del Cliente, y el Cliente es responsable de garantizar que dicha información de contacto se mantenga exacta y actualizada.

9. Asistencia al Cliente

9.1 Teniendo en cuenta la naturaleza del tratamiento, DeskTime prestará una asistencia razonable al Cliente para el cumplimiento de sus obligaciones conforme a las Leyes de Protección de Datos aplicables, incluido el apoyo técnico y organizativo adecuado en relación con la investigación de Violaciones de Datos Personales y las correspondientes obligaciones de notificación, la demostración del cumplimiento de las Leyes de Protección de Datos y, cuando proceda, la realización de evaluaciones de impacto relativas a la protección de datos y las consultas con las autoridades de control.

9.2 Si DeskTime recibe (i) cualquier solicitud de un Usuario Final relativa a los Datos Personales tratados durante la prestación de los Servicios (incluidas las solicitudes de acceso, rectificación, supresión, limitación, portabilidad o derechos similares), (ii) cualquier queja o reclamación relativa al tratamiento de Datos Personales, o (iii) cualquier orden, requerimiento, mandamiento u otra solicitud legal que exija la divulgación de Datos Personales, DeskTime lo notificará con prontitud al Cliente, salvo que la legislación aplicable lo prohíba.

9.3 DeskTime no responderá a dichas solicitudes, quejas o requerimientos legales sin la autorización previa del Cliente, salvo que esté obligada a hacerlo conforme a la legislación aplicable o por orden de una autoridad competente.

10. Auditoría

10.1 A solicitud por escrito del Cliente, DeskTime se compromete a proporcionar información suficiente para demostrar el cumplimiento de las obligaciones establecidas en este DPA y en las Leyes de Protección de Datos. Esta información se facilitará en la medida en que esté bajo el control de DeskTime, y siempre que DeskTime no tenga impedimento para divulgarla por disposición legal aplicable, deber de confidencialidad u otra obligación frente a terceros.

10.2 Si la información facilitada no resulta suficiente para confirmar el cumplimiento de este DPA por parte de DeskTime, DeskTime se compromete a permitir y contribuir a una auditoría de tratamiento de datos, siempre que dicha auditoría no implique la revisión de datos de terceros y que los registros y el acceso a la información en el marco de dicha auditoría se traten como información confidencial.

10.3 Dichas auditorías podrán ser realizadas por el Cliente o por auditores independientes autorizados por el Cliente. El Cliente asumirá los costes de dicha auditoría.

10.4 La auditoría se llevará a cabo en el momento acordado entre las partes, dentro del plazo de 1 mes desde que el Cliente haya solicitado la auditoría por escrito. El auditor deberá firmar un acuerdo de confidencialidad que incluya la obligación de no divulgar información comercial en su informe de auditoría, y el informe final también se facilitará a DeskTime. La auditoría se realizará durante el horario laboral habitual de DeskTime, sin interferir en sus actividades comerciales.

11. Vigencia y terminación

11.1 Este DPA entrará en vigor en el momento en que el Cliente acepte las Condiciones de Servicio de DeskTime y permanecerá en pleno vigor y efecto mientras el Cliente utilice los Servicios y disponga de una cuenta en DeskTime, y hasta que todos los Datos Personales hayan sido devueltos al Cliente o suprimidos de conformidad con lo dispuesto en este DPA o en las Leyes de Protección de Datos aplicables, momento en el que este DPA se extinguirá automáticamente, con excepción de las cláusulas que, por su naturaleza, deban permanecer en pleno vigor y efecto.

12. Disposiciones varias

12.1 DeskTime podrá modificar ocasionalmente este DPA, por ejemplo, cuando se introduzcan nuevos servicios o funciones. En caso de modificaciones o cambios, DeskTime informará al Cliente con la debida antelación mediante notificación electrónica dirigida al representante del Cliente, indicando la naturaleza y el alcance de las modificaciones, y otorgando al Cliente el derecho a rescindir los Servicios. Las modificaciones se aplicarán a partir del momento indicado en esta sección de la página web.

12.2 DeskTime no será responsable de las reclamaciones o quejas de los interesados relativas a cualquier actuación llevada a cabo por DeskTime conforme a las instrucciones recibidas del Cliente. El Cliente indemnizará y mantendrá indemne a DeskTime frente a todas las reclamaciones, responsabilidades, costes, gastos, pérdidas o daños (incluidas las pérdidas consecuentes, la pérdida de beneficios, la pérdida de reputación, todos los intereses, sanciones, costes legales y otros gastos profesionales) sufridos por DeskTime como consecuencia directa o indirecta del incumplimiento por parte del Cliente.

12.3 Este DPA se regirá por la legislación de la República de Letonia, y cualquier acción o procedimiento relacionado con este DPA (incluidos los derivados de controversias o reclamaciones extracontractuales) se someterá a los tribunales de la República de Letonia.

Si tiene alguna pregunta sobre estas Condiciones o sobre las prácticas de tratamiento de datos de DeskTime, póngase en contacto con nosotros por correo electrónico en support@desktime.com o a través de los siguientes datos de contacto:

SIA DeskTime

Delegado de Protección de Datos

Dirección: Riga, Ojāra Vācieša iela 6B, Letonia

ANEXO 1

Detalles del Tratamiento de Datos Personales

Este Anexo 1 forma parte del DPA e incluye los detalles del tratamiento de Datos Personales que DeskTime llevará a cabo por cuenta del Cliente.

Naturaleza y finalidad del tratamiento

DeskTime trata los Datos Personales de los Usuarios Finales por cuenta de los Clientes para prestar sus Servicios, incluidas la recopilación y el almacenamiento de datos sobre horas de trabajo, asistencia, tareas y actividad, la generación de informes y análisis, y la facilitación de funciones de gestión de Usuarios Finales, como el seguimiento de proyectos y la planificación del tiempo.

Categorías de interesados

Los empleados, representantes y demás Usuarios Finales del Cliente que estén registrados en la cuenta del Cliente.

Categorías de datos personales

En función del uso de los Servicios y de las funciones disponibles habilitadas por el Cliente, DeskTime podrá tratar los siguientes Datos Personales de los Usuarios Finales:

- Nombre completo, dirección de correo electrónico, contraseña, número de teléfono, fotografía
- Ubicación, zona horaria, hora de inicio y fin de la jornada laboral, duración de la jornada, tarifa por hora, tiempo sin conexión, tiempo dedicado a pausas, tiempo privado, calendario de ausencias, información sobre compañeros, capturas de pantalla del ordenador, información proporcionada en la herramienta de cálculo de costes de proyectos, número de pulsaciones de teclado o movimientos del ratón
- Dirección IP (incluida la dirección IP indicada por el Cliente como dirección IP del lugar de trabajo)
- Tipo de navegador, versión del software del navegador, nombres de las aplicaciones utilizadas, nombres de las tareas a realizar, sitios web visitados, versión del cliente de DeskTime, ruta de acceso a la aplicación
- Historial de comunicaciones, en caso de que se preste servicio de atención al cliente
- Otros datos que DeskTime pueda recibir durante la prestación del Servicio y que, en relación con otra información, puedan contener datos personales

Medidas técnicas y organizativas de seguridad

DeskTime mantiene un sistema de gestión de la seguridad de la información alineado con las mejores prácticas del sector y está certificado conforme a la norma ISO/IEC 27001, lo que garantiza un enfoque sistemático para la gestión y protección de la seguridad de la información.

1. Medidas de seguridad física

- El acceso físico a las instalaciones está restringido mediante mecanismos de control de entrada (por ejemplo, instalaciones cerradas, controles de acceso)
- Los derechos de acceso a las instalaciones se documentan y se revisan periódicamente
- Se aplican medidas adecuadas (por ejemplo, videovigilancia u otros controles equivalentes) para detectar y prevenir el acceso físico no autorizado

2. Seguridad de red y sistemas

- Se implementan y mantienen cortafuegos y controles de seguridad de red adecuados para proteger frente al acceso no autorizado
- Los sistemas se supervisan para detectar y prevenir amenazas cibernéticas y actividades no autorizadas
- Se aplica la segmentación de red y configuraciones seguras cuando procede

3. Cifrado y protección de datos

- Los Datos Personales se protegen mediante cifrado conforme a los estándares del sector, tanto en tránsito como en reposo, cuando procede
- Las claves de cifrado se gestionan de forma segura, incluyendo su rotación periódica y la restricción de su acceso

4. Control de acceso y autenticación

- El acceso a los sistemas y a los Datos Personales está restringido según el principio de necesidad de conocer y de mínimo privilegio
- Se implementan y revisan periódicamente los procesos de autenticación y gestión de acceso de los usuarios
- Los derechos de acceso se actualizan o revocan con prontitud cuando dejan de ser necesarios

5. Registro y supervisión

- El sistema de DeskTime y la actividad de acceso se registran para proporcionar un rastro de auditoría
- Los registros se revisan periódicamente para detectar anomalías, accesos no autorizados o incidentes de seguridad
- Se implementa una supervisión continua, cuando procede, para garantizar la seguridad y disponibilidad del sistema

6. Integridad y disponibilidad de los datos

- Se han implementado medidas para garantizar la integridad y exactitud de los Datos Personales
- Se realizan y comprueban copias de seguridad periódicas de los datos para garantizar su disponibilidad y recuperación
- Los sistemas se supervisan para detectar errores y garantizar la disponibilidad continua de los servicios

7. Medidas organizativas de seguridad

- Se establecen y mantienen políticas y procedimientos internos que regulan el tratamiento de datos y la seguridad de la información
- Los empleados reciben formación periódica en materia de seguridad y protección de datos
- El personal está sujeto a obligaciones de confidencialidad
- Las responsabilidades en materia de protección de datos y seguridad están claramente asignadas

8. Gestión de incidentes

- Se establece y mantiene un plan de respuesta a incidentes para detectar, responder y mitigar los incidentes de seguridad
- Los incidentes de seguridad se documentan y gestionan conforme a los procedimientos establecidos

9. Continuidad del negocio y gestión de riesgos

- Se implementan y prueban periódicamente planes de continuidad del negocio y recuperación ante desastres
- Se realizan evaluaciones de riesgos periódicas para identificar y mitigar los riesgos de seguridad
- Los sistemas informáticos y las medidas de continuidad se evalúan y actualizan periódicamente

10. Cumplimiento y revisión de la eficacia

- Las medidas de seguridad se someten a pruebas, evaluaciones y revisiones periódicas para comprobar su eficacia
- Se realizan auditorías y revisiones para garantizar el cumplimiento continuo de las Leyes de Protección de Datos aplicables
- Las medidas de seguridad se actualizan según sea necesario para hacer frente a los riesgos y estándares del sector en constante evolución