

Contrato de encargo de tratamiento de datos personales (DPA)

Última actualización: 15 de octubre de 2026

1. Partes y objeto

El presente contrato de encargo de tratamiento (en adelante, el "DPA") se celebra entre la organización cliente de la plataforma Utilia OS (en adelante, el "Responsable del tratamiento" o el "Cliente") y UTILIA SERVICIOS IA S. COOP. CAN., con NIF F75452102 y domicilio social en C/ Teniente Coronel Castillo Olivares, 26, piso 16, letra A-2, 35011 Las Palmas de Gran Canaria (en adelante, el "Encargado del tratamiento" o "UTILIA"), de conformidad con el artículo 28 del Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD).

El objeto del DPA es regular el tratamiento de datos personales que UTILIA realiza por cuenta del Responsable como consecuencia de la prestación del servicio de la plataforma Utilia OS, conforme al contrato de servicio suscrito entre las partes (los "Términos de uso" y, en su caso, el pedido o plan contratado).

2. Duración, naturaleza y finalidad del tratamiento

- Duración: el tratamiento se prolonga mientras esté vigente la relación de servicio entre el Cliente y UTILIA, más el periodo de devolución o supresión previsto en la cláusula 10 y, respecto de la documentación mercantil y tributaria, el plazo de conservación bloqueada que esa misma cláusula establece.

- Naturaleza: alojamiento, almacenamiento, estructuración, consulta, comunicación por transmisión, copia de seguridad, transcripción y análisis asistido por inteligencia artificial de los datos que el Cliente introduce en la plataforma, en la medida estrictamente necesaria para prestar cada funcionalidad activada por el Cliente.

- Finalidad: la prestación del servicio Utilia OS (CRM, finanzas y facturación, operaciones —compras, almacén y ventas—, comunicaciones internas, videoconferencia, gestión documental, gestión del trabajo, marketing, portal del cliente y demás módulos contratados), incluido el soporte técnico y el mantenimiento.

3. Tipo de datos personales y categorías de interesados

- Categorías de interesados: personal y colaboradores del Cliente; contactos comerciales, clientes finales y leads del Cliente; proveedores del Cliente que sean personas físicas y personas de contacto dentro de los proveedores del Cliente; usuarios del portal del cliente; participantes en reuniones, llamadas y comunicaciones gestionadas a través de la plataforma.

- Tipos de datos: datos identificativos y de contacto; datos profesionales y de empleo (incluidos el cargo y el área de las personas de contacto de los proveedores); datos económicos, financieros y de facturación (incluidos identificadores fiscales e IBAN cuando el Cliente los registra); contenido de comunicaciones, documentos y archivos; imágenes o fotografías de personas cuando el Cliente las incorpora a una ficha; registro de la actividad mantenida con esas personas (llamadas, correos, reuniones y notas) cuando el Cliente la anota; campos adicionales definidos por el propio Cliente para sus fichas, cuyo contenido decide él; documentos del ciclo de compras, almacén y ventas (solicitudes, pedidos, recepciones, albaranes, recuentos y movimientos de existencias), que registran la identidad de la persona usuaria que ejecuta cada paso y su fecha y hora; grabaciones y transcripciones de reuniones y llamadas cuando el Cliente activa esas funcionalidades; metadatos de uso técnico.

- La plataforma no está diseñada específicamente para tratar categorías especiales de datos del artículo 9 RGPD, pero algunas funcionalidades permiten tratarlas o tratar datos especialmente sensibles: en particular, el módulo de RRHH permite registrar ausencias cuyo tipo o motivo puede revelar datos de salud (como las bajas médicas, las citas médicas o la enfermedad de un familiar) y adjuntar sus justificantes, y, si el Cliente lo activa en su política de fichaje, registrar la ubicación de la persona al fichar. Corresponde al Cliente decidir si utiliza estas funcionalidades, determinar la base jurídica y, en su caso, la excepción del artículo 9.2 RGPD que ampara el tratamiento, y valorar su proporcionalidad. Si el Cliente decide introducir otras categorías especiales de datos bajo su responsabilidad, deberá contar con una base jurídica adecuada y comunicarlo a UTILIA para valorar medidas adicionales.

4. Obligaciones y derechos del Responsable

Corresponde al Responsable: (a) decidir sobre la finalidad, contenido y uso del tratamiento; (b) garantizar la licitud de los datos que introduce en la plataforma y la existencia de base jurídica; (c) atender los derechos de los interesados, con la asistencia de UTILIA descrita en la cláusula 8; (d) impartir instrucciones documentadas a UTILIA, siendo la configuración de la plataforma y las funcionalidades activadas la instrucción principal; y (e) velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte de UTILIA, ejerciendo la supervisión prevista en la cláusula 11.

5. Instrucciones documentadas (art. 28.3.a RGPD)

UTILIA tratará los datos personales únicamente siguiendo instrucciones documentadas del Responsable, incluidas las relativas a transferencias internacionales, salvo que una obligación del Derecho de la Unión o de un Estado miembro exija otro tratamiento; en tal caso, UTILIA informará al Responsable de esa exigencia legal antes del tratamiento, salvo que dicho Derecho lo prohíba por razones importantes de interés público. Si UTILIA considera que una instrucción infringe la normativa de protección de datos, informará inmediatamente al Responsable.

5 bis. Asistentes de inteligencia artificial conectados por las personas usuarias del Responsable

Las personas usuarias del Responsable pueden conectar a la plataforma asistentes de inteligencia artificial de terceros, como Claude, ChatGPT o Cursor, autorizándolos con su propia cuenta mediante OAuth o creando una clave personal. Las partes acuerdan que esa autorización o esa creación, realizada por una persona usuaria con las credenciales y los permisos que el Responsable le ha asignado, constituye una instrucción documentada del Responsable en el sentido del artículo 28.3.a) del RGPD para poner a disposición de esa aplicación los datos que solicite dentro de los permisos concedidos.

El proveedor del asistente es un destinatario elegido por el Responsable o por sus personas usuarias, en el sentido del artículo 4.9 del RGPD, y no un subencargado de UTILIA: UTILIA no lo contrata ni le encarga tratamiento alguno, y no recibe las conversaciones con el asistente, sino solo las peticiones que este formula a la plataforma. Corresponden al Responsable la base jurídica de esa comunicación de datos, el contrato o las condiciones que lo vinculen con ese proveedor y, en su caso, las garantías de las transferencias internacionales que este realice.

UTILIA registra en el registro de auditoría cada petición del asistente, incluidas las consultas, con la herramienta utilizada, sus parámetros (con los campos considerados sensibles ocultos por su nombre, como secretos, IBAN, NIF, teléfonos o coordenadas), la dirección IP y el programa que la formula, y la conserva durante el plazo de 365 días previsto para esa categoría en la política de retención del registro de auditoría. Conserva asimismo los datos de cada autorización (aplicación, persona, ámbitos concedidos, último uso y número de usos) hasta el día siguiente al fin de su plazo máximo de renovación, también cuando se retira antes, y registra en el registro de auditoría la creación y la retirada de claves personales y la desconexión de asistentes, con los plazos de esa misma política (cláusula 10.1).

El Responsable puede limitar el alcance de estos asistentes mediante el plan contratado, los permisos que asigna a cada persona usuaria, la exclusión de archivos y carpetas del acceso de la inteligencia artificial y la desactivación de personas usuarias, que retira todas sus conexiones. Cada persona usuaria puede retirar sus conexiones en cualquier momento.

6. Deber de confidencialidad (art. 28.3.b RGPD)

UTILIA garantiza que las personas autorizadas para tratar datos personales se han comprometido a respetar la confidencialidad o están sujetas a una obligación de confidencialidad de naturaleza estatutaria, y que reciben la formación necesaria en materia de protección de datos.

7. Medidas de seguridad (art. 28.3.c y art. 32 RGPD)

UTILIA aplica medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, entre ellas:

a) Cifrado de las comunicaciones y protección de las credenciales: cifrado de las comunicaciones mediante TLS; cifrado de los secretos y credenciales que los usuarios confían a la plataforma para sus integraciones; y conservación de las contraseñas, de los testigos de sesión y de los códigos de recuperación mediante resúmenes criptográficos, nunca en claro.

b) Control de acceso: permisos granulares con ámbitos de visibilidad por organización, departamento,

asignación o persona, que permiten aplicar el principio de mínimo privilegio; y verificación en dos pasos a disposición de todas las personas usuarias, mediante aplicación de autenticación de un solo uso, códigos de recuperación de un solo uso, confirmación desde la aplicación móvil con elección de un número entre tres opciones (diseñada para impedir que una aprobación se conceda por inercia), reconocimiento del teléfono de confianza en la aplicación móvil y, como alternativa activa salvo que el Responsable la desactive, código de un solo uso enviado por correo electrónico. La verificación en dos pasos es obligatoria para las personas con el rol de «Super Administrador» en la organización de UTILIA.

c) Gobierno de las sesiones: entrega del testigo de renovación en una cookie inaccesible desde el código de la página, acotada al propio sitio y a la ruta de autenticación; conservación de los testigos de las aplicaciones móviles en el llavero cifrado del dispositivo; consulta por cada persona usuaria de sus sesiones abiertas, con el dispositivo y la ubicación aproximada o la dirección IP, y cierre inmediato de cualquiera de ellas; cierre de sesiones por quien administra; bloqueo de la pantalla tras un periodo de inactividad en el navegador y en la aplicación de escritorio; y purga de los datos guardados en el aparato al cerrar sesión.

d) Detección y aviso: avisos a la persona usuaria ante los acontecimientos de seguridad de su cuenta (activación o retirada de la verificación en dos pasos, acceso desde un aparato no utilizado antes, rechazo de una solicitud de acceso desde la aplicación móvil y reinicio de la verificación por un administrador), con elección del canal por el que los recibe.

e) Aislamiento entre organizaciones clientes: separación lógica de los datos con políticas de seguridad aplicadas en la propia base de datos, además del filtrado por organización en la aplicación.

f) Trazabilidad: registro inmutable de auditoría de las acciones, encadenado mediante resúmenes criptográficos que hacen detectable cualquier alteración o supresión indebida, con los plazos de conservación de la cláusula 10.1.

g) Copias de seguridad: copias diarias de la base de datos, que se conservan catorce días, y un procedimiento documentado de prueba de su restauración.

Adicionalmente, UTILIA pone a disposición del Responsable medidas cuya activación y calibración corresponden a este, por ser quien conoce el riesgo de su propia actividad: la exigencia de la verificación en dos pasos a las personas que administran su cuenta; la desactivación del código de verificación enviado por correo electrónico; la duración del bloqueo por inactividad; el límite de exportaciones por hora; un modo restringido que congela las exportaciones y descargas masivas de los módulos y el acceso por la unidad de red sin interrumpir la consulta ordinaria, y que no impide la exportación completa de la organización, la creación de claves de acceso a la API, el uso de los asistentes de inteligencia artificial ya conectados ni la conexión de otros o la creación de claves personales para ellos; y una lista de dominios autorizados para los webhooks de las aplicaciones externas y para los servidores de correo propios. La activación o modificación de cualquiera de ellas, salvo la del límite de exportaciones, queda registrada en el registro de auditoría con la identidad de quien la decidió y el momento en que lo hizo.

8. Asistencia al Responsable (art. 28.3.e y 28.3.f RGPD)

UTILIA, teniendo en cuenta la naturaleza del tratamiento, asistirá al Responsable: (a) con medidas técnicas y organizativas apropiadas, en la atención de las solicitudes de ejercicio de los derechos de los interesados (acceso, rectificación, supresión, oposición, limitación, portabilidad y no ser objeto de decisiones individuales automatizadas); y (b) en el cumplimiento de las obligaciones de los artículos 32 a 36 del RGPD (seguridad, notificación de violaciones de seguridad a la autoridad de control y a los interesados, evaluaciones de impacto y consultas previas), teniendo en cuenta la información de que disponga. UTILIA notificará al Responsable, sin dilación indebida desde que tenga conocimiento, las violaciones de la seguridad de los datos personales que afecten a los datos tratados por cuenta del Responsable.

9. Subencargados (art. 28.2 y 28.3.d RGPD)

El Responsable autoriza de forma general la contratación de los subencargados incluidos en el listado público y versionado de subencargados de UTILIA, disponible en la página "Subencargados del tratamiento" de la plataforma (/legal/subprocesadores), que forma parte integrante de este DPA por referencia. UTILIA informará al Responsable de cualquier adición o sustitución de subencargados con al menos 30 días naturales de antelación, mediante un correo electrónico dirigido a la dirección de facturación de su cuenta o, en su defecto, a quien tenga en ella el rol de «Super Administrador», y mediante la actualización de esa página con la fecha de la revisión. Dentro de ese plazo, el Responsable podrá oponerse al cambio de forma motivada escribiendo a compliance@utilia.ai; si las partes no alcanzan una solución, el Responsable podrá resolver el contrato, sin penalización, con efectos anteriores a que el cambio se aplique a sus datos. UTILIA impone a cada subencargado, mediante contrato, las mismas obligaciones de protección de datos que las estipuladas en este DPA, en particular garantías suficientes de aplicación de medidas técnicas y

organizativas apropiadas, y responde ante el Responsable del cumplimiento de las obligaciones del subencargado. Las transferencias internacionales a subencargados fuera del Espacio Económico Europeo se amparan en el marco indicado para cada uno en dicho listado (Data Privacy Framework, Cláusulas Contractuales Tipo 2021/914 con evaluación de impacto de la transferencia, o decisión de adecuación).

10. Supresión o devolución al final del servicio (art. 28.3.g RGPD)

A la finalización de la prestación del servicio, UTILIA, a elección del Responsable, suprimirá o devolverá todos los datos personales tratados por su cuenta, y suprimirá las copias existentes, salvo que el Derecho de la Unión o de un Estado miembro exija su conservación. La plataforma ofrece mecanismos de exportación de datos para hacer efectiva la devolución, descritos en los Términos de uso: tras la baja, la cuenta se conserva durante noventa (90) días en modo de solo lectura para que el Responsable pueda exportar sus datos y, transcurrido ese plazo, UTILIA los suprime en un máximo de treinta (30) días adicionales. Los datos suprimidos pueden permanecer en las copias de seguridad hasta que estas se renueven; las copias diarias de la base de datos se conservan catorce (14) días.

Instrucción documentada sobre la documentación mercantil y tributaria. En cumplimiento del artículo 28.3, letras a) y g), del RGPD y del artículo 33 de la Ley Orgánica 3/2018, el Responsable imparte a UTILIA, al aceptar este DPA, la siguiente instrucción documentada sobre la documentación mercantil y tributaria que trata en Utilia OS (facturas; registros de facturación, libros registro y demás registros fiscales, incluidos los registros de las operaciones acogidas a los regímenes especiales de ventanilla única del Impuesto sobre el Valor Añadido, con la información utilizada para determinar el lugar de establecimiento, domicilio o residencia habitual de sus clientes; gastos y sus justificantes; asientos contables; declaraciones y autoliquidaciones con sus justificantes de presentación y pago; y cobros y pagos registrados; con los datos personales que contienen): (i) tras la baja, UTILIA la conservará bloqueada, en los términos del artículo 32 de la Ley Orgánica 3/2018, hasta el 31 de diciembre del décimo año siguiente al de la baja; (ii) durante el periodo de noventa (90) días posterior a la baja previsto en el párrafo anterior, el Responsable puede obtener una copia de esa documentación mediante la exportación de la plataforma, en formatos estructurados, de uso común y lectura mecánica; (iii) durante el bloqueo, UTILIA solo tratará esa documentación para ponerla a disposición de los jueces y tribunales, del Ministerio Fiscal, de las Administraciones Públicas competentes, incluidas las Administraciones tributarias de otros Estados miembros a través del Estado miembro de identificación, o del propio Responsable para atender sus requerimientos, y para su propia defensa frente a las responsabilidades derivadas de este encargo; y (iv) transcurrido el plazo, UTILIA la suprimirá de forma segura, incluidas sus copias de seguridad al término de su ciclo ordinario de rotación, y lo certificará a solicitud del Responsable. El Responsable puede modificar por escrito esta instrucción en cualquier momento, escribiendo a compliance@utilia.ai, y le corresponde comprobar que el plazo que instruya respeta sus obligaciones legales de conservación, en particular el plazo de diez (10) años, contados desde el final del año en que se realizó cada operación, del registro de las operaciones de los regímenes especiales de ventanilla única. Todo ello sin perjuicio de la excepción prevista en el subapartado 10.1 respecto del registro de auditoría, que tiene sus propios plazos. Para los Responsables que ya lo eran cuando se publicó esta versión, esta instrucción sustituye a la de la versión anterior desde que la acepten expresamente desde el aviso que muestra la plataforma o, si no lo hacen, una vez transcurridos treinta (30) días naturales completos desde su publicación, contados desde el día siguiente, en los mismos términos que el apartado 17 de los Términos de uso; hasta entonces, su documentación mercantil y tributaria se conserva bloqueada durante seis (6) años tras la baja, como preveía la versión que tenían aceptada.

10.1 Registro de auditoría y excepción al deber de supresión

Las partes reconocen que el registro de auditoría de la plataforma cumple una doble función. Respecto de los datos de negocio del Cliente, UTILIA actúa como encargado del tratamiento en los términos de este DPA. Respecto de los acontecimientos de seguridad de la plataforma, de la identificación de quien accede y de la trazabilidad de las operaciones, UTILIA actúa como responsable del tratamiento por cuenta propia, al amparo de los artículos 32 y 6.1.f) del RGPD, por tratarse de una medida de seguridad exigible al prestador y de la prueba de su propio cumplimiento conforme a los artículos 5.2 y 24 del RGPD.

En consecuencia, y como excepción a la obligación general de devolución o supresión de la cláusula 10 y del artículo 28.3.g) del RGPD, a la terminación del contrato UTILIA:

a) Pondrá a disposición del Cliente la exportación del registro de auditoría de su organización desde la plataforma, en formato CSV o JSON, mientras la cuenta siga accesible conforme a la cláusula 10, y le facilitará, a solicitud y dentro de los treinta días naturales siguientes, los asientos archivados que necesite para la formulación, el ejercicio o la defensa de reclamaciones o para acreditar su propio cumplimiento.

b) Conservará el registro de auditoría durante los plazos indicados en la política de retención vigente,

publicada en la documentación del servicio y en la Política de privacidad. Esos plazos se cuentan desde cada acontecimiento registrado. En la categoría relativa a la configuración de la empresa y a sus integraciones, que es la que sustenta la relación contractual, el archivo se conserva cinco años desde cada acontecimiento y, en todo caso, no se destruye hasta que hayan transcurrido cinco años desde la baja del Cliente, conforme al artículo 1964.2 del Código Civil. En la actividad de facturación, seis años desde cada acontecimiento, conforme al artículo 30 del Código de Comercio.

c) Durante ese período mantendrá los registros bloqueados en el sentido del artículo 32 de la Ley Orgánica 3/2018, sin tratamiento activo y con acceso limitado a la atención de requerimientos de jueces y tribunales, del Ministerio Fiscal, de las autoridades de protección de datos y de las Administraciones públicas competentes, así como a la formulación, el ejercicio y la defensa de reclamaciones. El archivo se guarda con bloqueo de objetos en modo de gobernanza, que impide modificarlo o borrarlo sin un permiso especial de administración, y con acceso restringido. Transcurrido el plazo procederá a su destrucción y emitirá certificado de destrucción a solicitud del Cliente, salvo que pese sobre los archivos un bloqueo legal en los términos de la letra e).

d) No atenderá instrucciones del Cliente de borrado anticipado del registro de auditoría, por resultar contrarias a la normativa de protección de datos en los términos del artículo 28.3, párrafo segundo, del RGPD, que obliga al encargado a informar de inmediato cuando una instrucción infringe dicha normativa. UTILIA informará al Cliente del plazo aplicable y de la fecha prevista de destrucción.

e) A solicitud del Cliente o por requerimiento de una autoridad competente, UTILIA aplicará un bloqueo legal sobre los archivos afectados, que impide su destrucción mientras no se levante expresamente.

Integridad. El registro se protege mediante una cadena de resúmenes criptográficos encadenados que permite detectar cualquier alteración o supresión de asientos.

11. Información y auditorías (art. 28.3.h RGPD)

UTILIA pondrá a disposición del Responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones de este DPA, y permitirá y contribuirá a la realización de auditorías e inspecciones por parte del Responsable o de un auditor autorizado por este, previa solicitud con antelación razonable, en horario laboral y sin acceso a datos de otras organizaciones clientes.

12. Responsabilidad y legislación aplicable

Cada parte responde de los daños causados por el tratamiento conforme a los artículos 82 a 84 del RGPD. Este DPA se rige por la legislación española y, para cualquier controversia derivada de él, las partes, con renuncia expresa a cualquier otro fuero que pudiera corresponderles, se someten a los Juzgados y Tribunales de Las Palmas de Gran Canaria, como establecen los Términos de uso.

13. Contacto

Para cualquier cuestión relativa a este DPA o al tratamiento de datos personales: compliance@utilia.ai.

