

Acuerdo de tratamiento de datos (DPA)

Última actualización: 1 de mayo de 2026 · Contrato conforme al art. 28 del RGPD.

Esta es una traducción facilitada solo a título informativo. Si hay diferencias entre esta traducción y la versión en inglés, prevalece la versión en inglés.

Cómo funciona

Este DPA forma parte de las condiciones de uso. Se activa automáticamente cuando se crea un espacio de trabajo y se guardan datos personales en él. La organización cliente propietaria del espacio de trabajo es el responsable del tratamiento; Dazr es el encargado del tratamiento. No hace falta firma; si tu proceso de compras necesita una copia firmada por ambas partes, escribe a legal@dazr.eu.

1. Definiciones

Los términos de este DPA tienen el significado que les da el Reglamento (UE) 2016/679 (el RGPD). Los «datos personales del cliente» son los datos personales que el responsable del tratamiento (o los miembros y auditores que actúan bajo su autoridad) introduce en el espacio de trabajo, incluidos los datos personales que figuren en tareas de control, evidencias, comentarios, archivos, riesgos, incidentes, fichas de proveedores, miembros e invitaciones, comunicaciones recibidas por el portal público y el registro de actividad.

2. Objeto, duración, naturaleza y finalidad

- Objeto: el tratamiento de los datos personales del cliente para que el responsable del tratamiento gestione su programa de cumplimiento en seguridad de la información y protección de datos con la plataforma Dazr Compliance.
- Duración: la vigencia de la suscripción del responsable del tratamiento, más el periodo de gracia posterior a la terminación previsto en las condiciones de uso.
- Naturaleza y finalidad: alojamiento, almacenamiento, transmisión, consulta, supresión y las operaciones descritas en las condiciones de uso y en la política de privacidad.
- Tipo de datos personales: datos identificativos de los miembros de los espacios de trabajo y de los auditores invitados (correo electrónico, nombre, rol); cuando proceda, datos identificativos de quienes informan a través del portal público y de quienes comunican incidentes; datos de contacto de empleadores y metadatos operativos que sube el responsable del tratamiento. El responsable del tratamiento se encarga de no subir categorías especiales de datos salvo que su propia base jurídica lo permita.
- Categorías de interesados: las personas empleadas, contratistas y auditores externos invitados del responsable del tratamiento, y cualquier persona identificada en los contenidos de cumplimiento que el responsable del tratamiento decida subir.

3. Obligaciones del encargado del tratamiento

1. Tratamos los datos personales del cliente únicamente siguiendo instrucciones documentadas del responsable del tratamiento. Esas instrucciones consisten en el uso de las funciones previstas de la plataforma; si consideramos que una instrucción infringe el RGPD u otra norma de protección de datos de la Unión o de los Estados miembros, lo comunicamos al responsable del tratamiento.
2. Garantizamos que las personas autorizadas para tratar los datos personales del cliente se han comprometido a respetar la confidencialidad.
3. Adoptamos todas las medidas exigidas por el art. 32 del RGPD (seguridad del tratamiento). Las medidas actuales se describen en la sección 7.
4. Respetamos las condiciones del art. 28, apartados 2 y 4, para recurrir a subencargados (véase la sección 6).
5. Teniendo en cuenta la naturaleza del tratamiento y la información de que disponemos, ayudamos al

responsable del tratamiento a atender las solicitudes de los interesados, a notificar violaciones de seguridad, a realizar evaluaciones de impacto y a realizar la consulta previa a las autoridades de control (art. 28, apartado 3, letras e y f).

6. A elección del responsable del tratamiento, al terminar la prestación de los servicios suprimimos o devolvemos todos los datos personales del cliente y suprimimos las copias existentes, salvo que el Derecho de la Unión o de los Estados miembros exija conservarlos.
7. Ponemos a disposición del responsable del tratamiento toda la información necesaria para demostrar el cumplimiento del art. 28 y permitimos y contribuimos a la realización de auditorías, incluidas inspecciones (véase la sección 9).

4. Obligaciones del responsable del tratamiento

- El responsable del tratamiento garantiza que cuenta con una base jurídica conforme al art. 6 (y, cuando proceda, al art. 9) para los datos personales que introduce en el espacio de trabajo.
- El responsable del tratamiento responde de la exactitud de los datos personales del cliente y de atender las solicitudes de los interesados sobre su espacio de trabajo (le remitimos las solicitudes que recibamos y le ayudamos según el art. 28, apartado 3, letra e).
- El responsable del tratamiento controla el acceso (roles de los miembros, invitaciones a auditores y el portal público de comunicación) mediante los ajustes de la plataforma.

5. Transferencias internacionales

Por defecto, los datos personales del cliente se almacenan en la Unión Europea. Cuando un subencargado tiene su sede fuera de la UE, las transferencias se rigen por las cláusulas contractuales tipo de la Comisión Europea (Decisión 2021/914), módulo 3 (de encargado a encargado), con las medidas complementarias descritas en la sección 7. Los subencargados actuales y su ubicación figuran en </legal/subprocessors>.

6. Subencargados del tratamiento

1. El responsable del tratamiento nos autoriza a recurrir a subencargados para prestar el servicio. La lista actual figura en </legal/subprocessors>.
2. Informamos al responsable del tratamiento de cualquier incorporación o sustitución prevista con al menos 30 días de antelación, mediante la suscripción por correo electrónico de esa página o por correo electrónico a la persona propietaria del espacio de trabajo.
3. El responsable del tratamiento puede oponerse por motivos razonables de protección de datos. Si no podemos atender la objeción, puede resolver el servicio afectado y recibir el reembolso proporcional de la parte no utilizada del periodo de facturación en curso.
4. Imponemos por contrato escrito a cada subencargado obligaciones de protección de datos que no protegen menos que las de este DPA, y seguimos respondiendo ante el responsable del tratamiento del cumplimiento de las obligaciones del subencargado.

7. Medidas de seguridad (art. 32)

- Cifrado. Los datos personales del cliente se cifran en reposo con AES-256-GCM en la capa de aplicación, además del cifrado del proveedor de almacenamiento. Todo el transporte se hace por HTTPS con HSTS precargado, sin alternativa sin cifrar. Las claves se derivan mediante HKDF de un secreto maestro que solo está en variables de entorno de la infraestructura de producción.
- Control de acceso. Control de acceso por roles en la plataforma (propietario, administrador, miembro, auditor); sesiones de auditor limitadas en el tiempo y revocables. El acceso operativo se limita a un pequeño equipo de soporte mediante el portal de soporte, que por diseño solo muestra metadatos.
- Autenticación. Inicio de sesión sin contraseña con código de un solo uso. Tokens de sesión firmados con

HMAC y de duración limitada. Limitación de solicitudes en cada punto de acceso público, incluido el inicio de sesión de administración.

- Resiliencia e integridad. Registro de actividad de solo adición de cada acción que cambia un estado. Copias de seguridad dentro de la UE. La integridad de los datos almacenados se verifica con etiquetas de autenticación AEAD; un texto cifrado alterado produce un error y no se sirve.
- Red y cabeceras. Content-Security-Policy estricta con una lista de permitidos de scripts en línea por hash, X-Frame-Options estricto, X-Content-Type-Options nosniff y HSTS precargado.
- Gestión de vulnerabilidades. Las dependencias tienen versiones fijas; seguimos los avisos de seguridad y aplicamos parches con un calendario acorde a su gravedad.

8. Violación de la seguridad de los datos personales

Si tenemos conocimiento de una violación de la seguridad que afecte a los datos personales del cliente, lo notificamos a la persona propietaria del espacio de trabajo sin dilación indebida y, a más tardar, 72 horas después de haber tenido conocimiento (art. 33, apartado 2). La notificación describe, en la medida en que se conozcan: la naturaleza de la violación, sus consecuencias probables, las medidas adoptadas o propuestas y el punto de contacto para obtener más información. Ayudamos al responsable del tratamiento a cumplir sus propias obligaciones de notificación de los arts. 33 y 34.

9. Auditorías

El responsable del tratamiento (o un auditor externo que designe) puede auditar nuestro cumplimiento de este DPA una vez cada doce meses, con un preaviso por escrito de al menos 30 días y en horario laboral, de forma que no perturbe indebidamente nuestras operaciones y respete la confidencialidad de los datos de otros clientes. Podemos cobrar una tarifa razonable por cualquier auditoría adicional. Cuando una obligación de auditoría del art. 28, apartado 3, letra h, pueda cumplirse con una certificación de un tercero de la que dispongamos, la facilitaremos en lugar de una auditoría presencial.

10. Responsabilidad

La responsabilidad de cada parte en virtud de este DPA está sujeta a los límites de las condiciones de uso. Esos límites no restringen la responsabilidad por los daños que sufran los interesados conforme al art. 82 del RGPD.

11. Duración y terminación

Este DPA se aplica mientras tratemos datos personales del cliente y sigue vigente tras la terminación de las condiciones de uso en la medida y durante el tiempo en que aún conservemos esos datos. Las secciones 8 (violaciones), 9 (auditorías) y 12 (devolución y supresión) siguen vigentes tras la terminación.

12. Devolución y supresión

Al terminar el servicio, el responsable del tratamiento puede exportar los datos del espacio de trabajo con las herramientas de exportación de la plataforma durante el periodo de gracia de 30 días de las condiciones de uso. Tras ese periodo suprimimos los datos personales del cliente; las copias de seguridad caducan según nuestro calendario de conservación. Los datos que debemos conservar (por ejemplo, la facturación conforme al Derecho mercantil italiano) solo se conservan durante el plazo de esa obligación.

13. Orden de prelación

Si hay un conflicto entre este DPA y las condiciones de uso o la política de privacidad, este DPA prevalece en materia de tratamiento de datos. Las cláusulas contractuales tipo incorporadas para una transferencia fuera de la UE prevalecen sobre este DPA y sobre las condiciones de uso en lo que regulan.

14. Notificaciones

- A Dazr: privacy@dazr.eu (protección de datos) o security@dazr.eu (incidentes).
- Al responsable del tratamiento: el correo electrónico de la persona propietaria del espacio de trabajo que conste en el momento de la notificación.