REGISTRO DE ACTIVIDADES DE TRATAMIENTO COMO RESPONSABLE

Reglamento (UE) 2016/679 · LOPDGDD (LO 3/2018) · Artículo 30 RGPD

1. Identificación del responsable del tratamiento

NOMBRE EMPRESA	*Enfasys Ingeniería S.L.*

CIF	*B52572757*

DIRECCIÓN	*Calle Profesor Potter 183, Edificio Vorágine,33203, Gijón, Asturias.*

DPD / DELEGADO DE PROTECCIÓN DE DATOS	*dpo@excell.es*

2. Resumen de actividades de tratamiento

Código	Actividad de tratamiento	Base jurídica principal
T-01	*Gestión de personal RR.HH*	*Art. 6.1.b y 6.1.c RGPD*
T-02	*Gestión comercial y de clientes (B2B)*	*Art. 6.1.b RGPD*
T-03	*Gestión de proveedores y suministradores*	*Art. 6.1.b RGPD*
T-05	*Prevención de riesgos laborales (PRL)*	*Art. 6.1.c RGPD*
T-06	*Ejercicio de derechos conforme al RGPD*	*Art. 6.1.c RGPD*
T-07	*Gestión comercial / marketing*	*Art. 6.1.a y 6.1.f RGPD*
T-08	*Consultas y contacto (web / email / teléfono)*	*Art. 6.1.b RGPD*
T-10	*Gestión de brechas de seguridad*	*Art. 6.1.c RGPD*
T-11	*Gestión administrativa, económica y presupuestaria*	*Art. 6.1.c RGPD*
T-13	*Uso de inteligencia artificial (IA)*	*Art. 6.1.b / 6.1.c / 6.1.f RGPD (según uso)*

Elaboración inicial del RAT (T-01 a T-13)

Excell Compliance S.L.

T-01 Gestión de personal - RR.HH

Identificación del tratamiento	Nombre y finalidad
Nombre	*Gestión de personal*
Descripción finalidad	*Gestión del ciclo laboral de los empleados: contratación, control de presencia, nóminas, Seguridad Social, bajas y altas, control de vacaciones y permisos.*

Licitud del tratamiento
El tratamiento de datos se basa en el artículo 6.1 b) del RGPD para la ejecución de un contrato (contrato laboral), así como en el artículo 6.1 c) del RGPD para el cumplimiento de una obligación legal aplicable al Responsable del Tratamiento de acuerdo con:
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- Ley 35/2006, de 28 de noviembre, de Impuesto sobre la Renta de las Personas Físicas.
- Ley General de la Seguridad Social (RDL 8/2015, de 30 de octubre).
El tratamiento de las categorías especiales de datos de salud se realiza de acuerdo con el artículo 9.2 b) del RGPD relacionado con la legislación en materia de personal.

Plazos de conservación
4 años (obligaciones tributarias) / 5 años (obligaciones laborales y SS). Documentación contable: 6 años (art. 30 Código de Comercio). CVs de candidatos no seleccionados: máximo 1 año desde la finalización del proceso de selección.

Descripción del tratamiento	
Origen y procedencia de los datos	*La persona interesada.*
Colectivos afectados	*Empleados y ex-empleados de la empresa. Candidatos en procesos de selección.*

Categorías de datos tratados	
Tipologías de datos	
Infracciones	*n/a*
Categorías especiales de datos	*Salud (bajas médicas, aptitud laboral).*
Datos identificativos	*Nombre y apellidos; número de la Seguridad Social; DNI/NIF; dirección; email; teléfono; imagen; firma.*
Otros	*Datos académicos; datos de empleo; datos bancarios (IBAN para nómina); financieros y de seguros. Control de presencia y horario mediante App móvil.*

Medidas de seguridad
Acceso restringido al personal de RRHH y administración.
Gestión de nóminas externalizada a Asergrup / Koala (encargado del tratamiento).
Control horario mediante App móvil.
Control de acceso por usuario y contraseña con política de contraseñas corporativa.
Autenticación de doble factor (2FA) en acceso a sistemas con datos personales.
Cifrado de disco en equipos informáticos.
Antivirus y firewall activos en todos los equipos.
Copias de seguridad diaria almacenadas en servidor externo.
Copias de seguridad cifradas.
Compromisos de confidencialidad firmados por todo el personal con acceso a datos personales.

Procedimiento documentado para atender el ejercicio de derechos RGPD.
Registro de accesos a sistemas con datos personales.

Comunicaciones de datos

Están previstas comunicaciones cuando se pueda realizar la comunicación de datos conforme al artículo 6 del RGPD a:
- Asergrup / Koala: gestoría laboral encargada del tratamiento de nóminas.
- Tesorería General de la Seguridad Social (TGSS).
- Agencia Estatal de Administración Tributaria (AEAT).
- Entidades bancarias para el abono de nóminas
- Mutua de accidentes de trabajo y enfermedades profesionales

Transferencia internacional de datos

Transferencias Internacionales de datos

No están previstas transferencias internacionales de datos. El proveedor de software de RRHH/nóminas tiene sede en la UE (EEE).

T-02 Gestión comercial y de clientes - B2B

Identificación del tratamiento	Nombre y finalidad
Nombre	*Gestión comercial y de clientes (B2B)*
Descripción finalidad	*Gestión de las relaciones comerciales con empresas clientes: presupuestos, pedidos, facturación, cobros y comunicaciones comerciales. Base de datos aproximada: 20 contactos/empresas.*

Licitud del tratamiento
El tratamiento de datos se basa en el artículo 6.1 b) del RGPD para la ejecución de un contrato de suministro, así como en el artículo 6.1 c) del RGPD para el cumplimiento de obligaciones legales de facturación y contabilidad, de acuerdo con: *- Real Decreto de 22 de agosto de 1885 por el que se publica el Código de Comercio (art. 30).* *- Ley 58/2003, de 17 de diciembre, General Tributaria (art. 66-70).* *- Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido.*

Plazos de conservación
6 años desde la última factura de acuerdo con el artículo 30 del Código de Comercio y artículo 66 de la Ley General Tributaria.

Descripción del tratamiento	
Origen y procedencia de los datos	*La empresa cliente o la persona de contacto interesada.*
Colectivos afectados	*Personas de contacto (nombre, cargo, email, teléfono) en empresas clientes. Total aproximado: 20 empresas en la base de datos.*

Categorías de datos tratados	
Tipologías de datos	
Infracciones	*n/a*
Categorías especiales de datos	*n/a*
Datos identificativos	*Nombre y apellidos; cargo; email profesional; teléfono; firma.*
Otros	*Datos de la empresa (razón social, CIF, dirección); datos económicos (condiciones comerciales, historial de pedidos, facturas). Gestionado mediante Holded (sede UE).*

Medidas de seguridad
Software de gestión: Holded (sede UE). Acceso restringido al personal comercial y de administración. *Control de acceso por usuario dentro del software de gestión.* *Control de acceso por usuario y contraseña con política de contraseñas corporativa.* *Autenticación de doble factor (2FA) en acceso a sistemas con datos personales.* *Cifrado de disco en equipos informáticos.* *Antivirus y firewall activos en todos los equipos.* *Copias de seguridad diaria almacenadas en servidor externo.* *Copias de seguridad cifradas.* *Compromisos de confidencialidad firmados por todo el personal con acceso a datos personales.* *Procedimiento documentado para atender el ejercicio de derechos RGPD.* *Registro de accesos a sistemas con datos personales.*

Comunicaciones de datos

Están previstas comunicaciones cuando se pueda realizar la comunicación de datos conforme al artículo 6 del RGPD a:

- Agencia Estatal de Administración Tributaria (AEAT) (IVA, declaraciones).

- Entidades bancarias para la gestión de cobros

- Holded: proveedor de software de gestión (encargado del tratamiento).

- Auditores externos o asesores cuando proceda.

Transferencia internacional de datos

Transferencias Internacionales de datos

No están previstas transferencias internacionales de datos. El proveedor de software (Holded) tiene sede en la Unión Europea (EEE).

T-03 Gestión de proveedores - y suministradores

Identificación del tratamiento	Nombre y finalidad
Nombre	*Gestión de proveedores y suministradores*
Descripción finalidad	*Gestión de las relaciones con proveedores de bienes y servicios, incluyendo autónomos suministradores. Base de datos aproximada: 2 proveedores/autónomos.*

Licitud del tratamiento
El tratamiento de datos se basa en el artículo 6.1 b) del RGPD para la ejecución del contrato de compraventa o prestación de servicios, así como en el artículo 6.1 c) del RGPD para el cumplimiento de obligaciones legales de acuerdo con: *- Real Decreto de 22 de agosto de 1885 (Código de Comercio, art. 30).* *- Ley 58/2003, de 17 de diciembre, General Tributaria (art. 66-70).* *- Ley 35/2006, de 28 de noviembre, del IRPF: retenciones a profesionales autónomos (modelo 190/111).*

Plazos de conservación
6 años desde la última factura, de acuerdo con el artículo 30 del Código de Comercio y el artículo 66 de la Ley General Tributaria.

Descripción del tratamiento	
Origen y procedencia de los datos	*La empresa proveedora o el autónomo interesado.*
Colectivos afectados	*Personas de contacto en empresas proveedoras y autónomos suministradores de bienes y servicios.*

Categorías de datos tratados	
Tipologías de datos	
Infracciones	*n/a*
Categorías especiales de datos	*n/a*
Datos identificativos	*Nombre y apellidos; DNI/NIF (para autónomos y personas físicas); email; teléfono; firma.*
Otros	*Datos de la empresa proveedora (razón social, CIF, dirección); datos económicos (condiciones de compra, facturas, IBAN para pagos). Contratos conservados en formato digital. Gestionado mediante Holded (mismo que T-02).*

Medidas de seguridad
Software de gestión: Holded (mismo que T-02). Acceso restringido al personal de compras y administración. *Control de acceso por usuario y contraseña con política de contraseñas corporativa.* *Autenticación de doble factor (2FA) en acceso a sistemas con datos personales.* *Cifrado de disco en equipos informáticos.* *Antivirus y firewall activos en todos los equipos.* *Copias de seguridad diaria almacenadas en servidor externo.* *Copias de seguridad cifradas.* *Compromisos de confidencialidad firmados por todo el personal con acceso a datos personales.* *Procedimiento documentado para atender el ejercicio de derechos RGPD.* *Registro de accesos a sistemas con datos personales.*

Comunicaciones de datos
Están previstas comunicaciones cuando se pueda realizar la comunicación de datos conforme al artículo 6 del RGPD a: *- Agencia Estatal de Administración Tributaria (AEAT): modelos de retención (111/190) y declaración de operaciones con terceros (347).* *- Entidades bancarias para la gestión de pagos: [PENDIENTE — completar por el cliente].* *- Holded: proveedor de software de gestión (encargado del tratamiento).*

Transferencia internacional de datos
Transferencias Internacionales de datos
No están previstas transferencias internacionales de datos.

T-05 Prevención de Riesgos Laborales - PRL y vigilancia de la salud

Identificación del tratamiento	**Nombre y finalidad**
Nombre	*Prevención de Riesgos Laborales (PRL)*
Descripción finalidad	*Gestión de la seguridad y salud en el trabajo: vigilancia de la salud de los empleados, gestión de accidentes laborales, evaluaciones de riesgo, planificación preventiva y formación en PRL.*

Licitud del tratamiento
El tratamiento de datos se basa en el artículo 6.1 c) del RGPD (obligación legal) y el artículo 9.2 b) del RGPD para los datos de salud, de conformidad con: *- Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales (LPRL, art. 22 y 23).* *- Real Decreto 39/1997, de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención (RSP, art. 37.3).*

Plazos de conservación
Durante la relación laboral más 5 años (LPRL, art. 23). Los historiales médicos son accesibles exclusivamente por el SPA.

Descripción del tratamiento	
Origen y procedencia de los datos	*La persona interesada (empleado) y el Servicio de Prevención Ajeno.*
Colectivos afectados	*Empleados de la empresa.*

Categorías de datos tratados	
Tipologías de datos	
Infracciones	*n/a*
Categorías especiales de datos	*Datos de salud: resultados de reconocimientos médicos, aptitud laboral. CATEGORÍA ESPECIAL (art. 9 RGPD).*
Datos identificativos	*Nombre y apellidos; DNI/NIF; número de la Seguridad Social; datos de contacto.*
Otros	*Datos laborales (puesto de trabajo, categoría profesional, antigüedad); datos de formación en PRL; registro de evaluaciones de riesgo y planificaciones preventivas (conservadas en formato digital).*

Medidas de seguridad
Servicio de Prevención Ajeno (SPA): Los datos de salud son accesibles exclusivamente por el personal médico del SPA. *Acceso muy restringido. Cifrado de expedientes médicos.* *Control de acceso por usuario y contraseña con política de contraseñas corporativa.* *Autenticación de doble factor (2FA) en acceso a sistemas con datos personales.* *Cifrado de disco en equipos informáticos.* *Antivirus y firewall activos en todos los equipos.* *Copias de seguridad diaria almacenadas en servidor externo.* *Copias de seguridad cifradas.* *Compromisos de confidencialidad firmados por todo el personal con acceso a datos personales.* *Procedimiento documentado para atender el ejercicio de derechos RGPD.* *Registro de accesos a sistemas con datos personales.*

Comunicaciones de datos
Están previstas comunicaciones cuando se pueda realizar la comunicación de datos conforme al artículo 6 del RGPD a: *- Servicio de Prevención Ajeno: [PENDIENTE — completar por el cliente] (encargado del tratamiento).* *- Mutua de accidentes de trabajo y enfermedades profesionales: [PENDIENTE — completar por el cliente].* *- Inspección de Trabajo y Seguridad Social (cuando lo requiera).* *- Instituto Nacional de la Seguridad Social (INSS) en caso de accidente laboral.*

Transferencia internacional de datos
Transferencias Internacionales de datos
No están previstas transferencias internacionales de datos.

T-06 Ejercicio de derechos - conforme al RGPD

Identificación del tratamiento	Nombre y finalidad
Nombre	*Ejercicio de derechos conforme al RGPD*
Descripción finalidad	*Gestión y tramitación de las solicitudes ejercitadas por los interesados en relación con sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad de los datos (artículos 15 a 22 del RGPD).*

Licitud del tratamiento
El tratamiento de datos se basa en el artículo 6.1 c) del RGPD (obligación legal) de conformidad con: *- Artículos 15 a 22 del Reglamento (UE) 2016/679 (RGPD), que reconocen los derechos de los interesados.* *- Artículos 13 a 18 de la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), que desarrollan dichos derechos.* *- Artículo 12 del RGPD: el responsable debe responder en el plazo máximo de 1 mes desde la recepción de la solicitud (prorrogable a 3 meses en casos complejos).*

Plazos de conservación
3 años desde la resolución de la solicitud, de acuerdo con el artículo 12 de la LOPDGDD (plazo de prescripción de infracciones muy graves).

Descripción del tratamiento	
Origen y procedencia de los datos	*La persona interesada que ejerce su derecho.*
Colectivos afectados	*Cualquier interesado cuyos datos trate la empresa: empleados, clientes, proveedores, candidatos u otras personas.*

Categorías de datos tratados	
Tipologías de datos	
Infracciones	*n/a*
Categorías especiales de datos	*Las que correspondan según el derecho ejercitado y el tratamiento afectado.*
Datos identificativos	*Nombre y apellidos; DNI/NIF (para verificación de identidad); dirección o email de contacto.*
Otros	*Descripción de la solicitud presentada; documentación aportada por el solicitante; respuesta y resolución emitida; fecha de recepción y de resolución.*

Medidas de seguridad
Registro documentado de cada solicitud y su respuesta. *Verificación de la identidad del solicitante antes de atender la solicitud.* *Acceso restringido al responsable de protección de datos o persona designada.* *Control de acceso por usuario y contraseña con política de contraseñas corporativa.* *Autenticación de doble factor (2FA) en acceso a sistemas con datos personales.* *Cifrado de disco en equipos informáticos.* *Antivirus y firewall activos en todos los equipos.* *Copias de seguridad diaria almacenadas en servidor externo.* *Copias de seguridad cifradas.* *Compromisos de confidencialidad firmados por todo el personal con acceso a datos personales.* *Procedimiento documentado para atender el ejercicio de derechos RGPD.*

Registro de accesos a sistemas con datos personales.

Comunicaciones de datos

No están previstas cesiones de datos a terceros en el contexto de este tratamiento.

- Si se designa DPD, puede intervenir en la tramitación.

- La Agencia Española de Protección de Datos (AEPD) puede recibir reclamaciones si el derecho no es atendido.

Transferencia internacional de datos

Transferencias Internacionales de datos

No están previstas transferencias internacionales de datos.

T-07 Gestión comercial - y marketing

Identificación del tratamiento	Nombre y finalidad
Nombre	*Gestión comercial y marketing*
Descripción finalidad	*Envío de comunicaciones comerciales, promociones y acciones de marketing dirigidas a clientes actuales y potenciales por correo electrónico. Destinatarios: nuevos contactos captados e interés legítimo sobre clientes existentes.*

Licitud del tratamiento
El tratamiento de datos se basa en: *- Artículo 6.1 a) del RGPD (consentimiento del interesado) para nuevos contactos captados.* *- Artículo 6.1 f) del RGPD (interés legítimo) para el envío de comunicaciones a clientes existentes en el marco del artículo 21.2 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).* *OBLIGACIÓN (art. 21 LSSI): toda comunicación comercial por email debe identificar al remitente e incluir mecanismo sencillo y gratuito de baja.*

Plazos de conservación
Hasta que el interesado retire el consentimiento o ejerza el derecho de oposición. Máximo 3 años desde el último contacto comercial activo.

Descripción del tratamiento	
Origen y procedencia de los datos	*La persona interesada (cliente, contacto comercial).*
Colectivos afectados	*Clientes actuales y potenciales (B2B). Contactos captados en acciones comerciales.*

Categorías de datos tratados	
Tipologías de datos	
Infracciones	*n/a*
Categorías especiales de datos	*n/a*
Datos identificativos	*Nombre y apellidos; cargo; email profesional; teléfono.*
Otros	*Datos de la empresa (razón social, sector); historial de comunicaciones comerciales; preferencias e intereses. Plataforma de email marketing:*

Medidas de seguridad
Gestión de listas de exclusión (opt-out). *Registro de consentimientos obtenidos con fecha y medio.* *Enlace de baja (unsubscribe) incluido en cada comunicación comercial.* *Contrato de encargo con la plataforma de email marketing* *Control de acceso por usuario y contraseña con política de contraseñas corporativa.* *Autenticación de doble factor (2FA) en acceso a sistemas con datos personales.* *Cifrado de disco en equipos informáticos.* *Antivirus y firewall activos en todos los equipos.* *Copias de seguridad diaria almacenadas en servidor externo.* *Copias de seguridad cifradas.* *Compromisos de confidencialidad firmados por todo el personal con acceso a datos personales.*

Procedimiento documentado para atender el ejercicio de derechos RGPD.

Registro de accesos a sistemas con datos personales.

Comunicaciones de datos

Están previstas comunicaciones cuando se pueda realizar la comunicación de datos conforme al artículo 6 del RGPD a:

- Plataforma de email marketing utilizada:

No se ceden datos a terceros con fines comerciales.

Transferencia internacional de datos

Transferencias Internacionales de datos

T-08 Consultas y contacto - web, email y teléfono

Identificación del tratamiento	Nombre y finalidad
Nombre	*Consultas y contacto (web, email y teléfono)*
Descripción finalidad	*Gestión de las consultas, solicitudes de información, peticiones de presupuesto y comunicaciones recibidas a través de los canales de contacto de la empresa: formulario web, correo electrónico, teléfono u otros medios.*

Licitud del tratamiento
El tratamiento de datos se basa en: *- Artículo 6.1 b) del RGPD para la aplicación de medidas precontractuales a solicitud del interesado.* *- Artículo 6.1 a) del RGPD (consentimiento) cuando el contacto no tiene finalidad contractual directa.* *La página web incluye enlace visible a la Política de Privacidad y casilla de aceptación en el formulario de contacto, de conformidad con el artículo 13 del RGPD. Estado actual: Política de privacidad actualizada; formulario con cláusula y checkbox RGPD.*

Plazos de conservación
1 año desde la atención de la consulta si no deriva en relación contractual. Si deriva en relación comercial, se aplicará el plazo del T-02 (6 años).

Descripción del tratamiento	
Origen y procedencia de los datos	*La persona física o representante de empresa que realiza el contacto.*
Colectivos afectados	*Cualquier persona física o representante de empresa que contacte con la organización a través de cualquier canal disponible.*

Categorías de datos tratados	
Tipologías de datos	
Infracciones	*n/a*
Categorías especiales de datos	*n/a*
Datos identificativos	*Nombre y apellidos; empresa; email; teléfono.*
Otros	*Contenido del mensaje o consulta; datos relativos al interés o necesidad manifestada.*

Medidas de seguridad
Cláusula informativa visible en el formulario de contacto web. *Cifrado de las comunicaciones por email (protocolo TLS).* *Acceso restringido al personal que gestiona las consultas.* *Proveedor de hosting web: Ionos (sede EEE)* *Control de acceso por usuario y contraseña con política de contraseñas corporativa.* *Autenticación de doble factor (2FA) en acceso a sistemas con datos personales.* *Cifrado de disco en equipos informáticos.* *Antivirus y firewall activos en todos los equipos.* *Copias de seguridad diaria almacenadas en servidor externo.* *Copias de seguridad cifradas.* *Compromisos de confidencialidad firmados por todo el personal con acceso a datos personales.* *Procedimiento documentado para atender el ejercicio de derechos RGPD.*

Registro de accesos a sistemas con datos personales.

Comunicaciones de datos

No están previstas cesiones de datos a terceros.

- El área correspondiente (comercial, técnico, administración) recibe la consulta internamente.

- Proveedor de hosting web: Ionos (encargado del tratamiento).

Transferencia internacional de datos

Transferencias Internacionales de datos

No están previstas transferencias internacionales de datos. Verificar la ubicación del proveedor de hosting (Ionos) y confirmar que el procesamiento se realiza en el EEE.

T-10 Gestión de brechas de seguridad - violaciones de datos personales

Identificación del tratamiento	Nombre y finalidad
Nombre	*Gestión de brechas de seguridad*
Descripción finalidad	*Detección, registro, análisis, notificación y seguimiento de las violaciones de seguridad de los datos personales (brechas) que puedan afectar a la confidencialidad, integridad o disponibilidad de los datos tratados por la empresa.*

Licitud del tratamiento
El tratamiento de datos se basa en el artículo 6.1 c) del RGPD (obligación legal) de conformidad con: *- Artículo 33 del RGPD: obligación de notificar las brechas a la autoridad de control (AEPD) en el plazo máximo de 72 horas desde su conocimiento.* *- Artículo 34 del RGPD: obligación de comunicar la brecha a los interesados cuando el riesgo sea alto.* *- Artículo 33.5 del RGPD: obligación de documentar todas las brechas de seguridad, incluso las no notificadas.* *PLAZO CRÍTICO: la notificación a la AEPD debe realizarse en el plazo máximo de 72 horas desde el conocimiento de la brecha.*

Plazos de conservación
El registro interno de violaciones de seguridad debe conservarse de forma indefinida, de acuerdo con el artículo 33.5 del RGPD.

Descripción del tratamiento	
Origen y procedencia de los datos	*Detección interna o notificación de encargados del tratamiento o terceros.*
Colectivos afectados	*Empleados, clientes, proveedores o cualquier persona cuyos datos hayan podido verse comprometidos.*

Categorías de datos tratados	
Tipologías de datos	
Infracciones	*Pueden incluirse datos relativos a posibles infracciones si la brecha está relacionada con accesos no autorizados o actos ilícitos.*
Categorías especiales de datos	*Las que correspondan según los datos afectados por la brecha de seguridad.*
Datos identificativos	*Datos de los interesados afectados por la brecha (según el tipo de tratamiento implicado).*
Otros	*Descripción y alcance de la brecha; fecha de detección; categorías y volumen de datos afectados; consecuencias estimadas; medidas correctoras adoptadas; fecha y contenido de las notificaciones realizadas.*

Medidas de seguridad
Procedimiento documentado de gestión de incidentes de seguridad. *Registro interno de todas las brechas (incluso las no notificadas).* *Evaluación del riesgo para determinar la necesidad de notificación.* *Acceso muy restringido al registro de brechas.* *Control de acceso por usuario y contraseña con política de contraseñas corporativa.* *Autenticación de doble factor (2FA) en acceso a sistemas con datos personales.* *Cifrado de disco en equipos informáticos.* *Antivirus y firewall activos en todos los equipos.* *Copias de seguridad diaria almacenadas en servidor externo.*

Copias de seguridad cifradas.

Compromisos de confidencialidad firmados por todo el personal con acceso a datos personales.

Procedimiento documentado para atender el ejercicio de derechos RGPD.

Registro de accesos a sistemas con datos personales.

Comunicaciones de datos

Están previstas comunicaciones cuando se pueda realizar la comunicación de datos conforme al artículo 6 del RGPD a:

- Agencia Española de Protección de Datos (AEPD) cuando la brecha suponga riesgo para los derechos y libertades (plazo: 72 horas, art. 33 RGPD).

- Interesados afectados cuando el riesgo sea alto (art. 34 RGPD).

- Responsable de protección de datos designado.

Transferencia internacional de datos

Transferencias Internacionales de datos

No están previstas transferencias internacionales de datos.

T-11 Gestión administrativa - económica y presupuestaria

Identificación del tratamiento	Nombre y finalidad
Nombre	*Gestión administrativa, económica y presupuestaria*
Descripción finalidad	*Gestión de la contabilidad general, presupuestaria y financiera de la empresa: registro contable, control de tesorería, gestión bancaria, elaboración de presupuestos, reporting interno y cumplimiento de obligaciones fiscales y mercantiles.*

Licitud del tratamiento
El tratamiento de datos se basa en el artículo 6.1 c) del RGPD (obligación legal) de conformidad con: *- Real Decreto de 22 de agosto de 1885, Código de Comercio (art. 25 y 30): obligación de llevanza de contabilidad.* *- Ley 58/2003, de 17 de diciembre, General Tributaria (LGT), y normativa de desarrollo.* *- Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba la Ley de Sociedades de Capital (LSC).*

Plazos de conservación
Libros contables y documentación justificante: 6 años desde el cierre del ejercicio (Código de Comercio, art. 30). Obligaciones tributarias: 4 años (LGT, art. 66). Documentación societaria (estatutos, actas): conservación permanente.

Descripción del tratamiento	
Origen y procedencia de los datos	*La propia empresa, clientes, proveedores y entidades financieras.*
Colectivos afectados	*Personas físicas que sean clientes (autónomos, empresarios individuales) o proveedores autónomos. Empleados en la parte contable de nóminas.*

Categorías de datos tratados	
Tipologías de datos	
Infracciones	*n/a*
Categorías especiales de datos	*n/a*
Datos identificativos	*Nombre y apellidos; DNI/NIF (para autónomos y personas físicas); dirección; email.*
Otros	*Datos bancarios (número de cuenta, IBAN); datos económicos (facturas, importes, condiciones pactadas); datos contables y presupuestarios.*

Medidas de seguridad
Acceso restringido al personal de administración y finanzas. *Software contable con control de acceso y trazabilidad de operaciones.* *Control de acceso por usuario y contraseña con política de contraseñas corporativa.* *Autenticación de doble factor (2FA) en acceso a sistemas con datos personales.* *Cifrado de disco en equipos informáticos.* *Antivirus y firewall activos en todos los equipos.* *Copias de seguridad diaria almacenadas en servidor externo.* *Copias de seguridad cifradas.* *Compromisos de confidencialidad firmados por todo el personal con acceso a datos personales.* *Procedimiento documentado para atender el ejercicio de derechos RGPD.* *Registro de accesos a sistemas con datos personales.*

Comunicaciones de datos

Están previstas comunicaciones cuando se pueda realizar la comunicación de datos conforme al artículo 6 del RGPD a:

- Agencia Estatal de Administración Tributaria (AEAT).

- Entidades bancarias.

- Auditores externos (si procede).

- Gestoría / asesoría contable y fiscal: Asergrup / Koala (encargado del tratamiento).

Transferencia internacional de datos

Transferencias Internacionales de datos

No están previstas transferencias internacionales de datos.

T-13 Uso de Inteligencia Artificial - IA generativa y sistemas automatizados

Identificación del tratamiento	**Nombre y finalidad**
Nombre	*Uso de Inteligencia Artificial (IA)*
Descripción finalidad	*Tratamiento de datos personales en el contexto de la utilización de herramientas, sistemas o servicios basados en inteligencia artificial (IA) para tareas de la empresa: asistentes de escritura, análisis de datos, automatización de procesos u otras aplicaciones. Herramientas utilizadas: [PENDIENTE — completar por el cliente]. Usos: [PENDIENTE — completar por el cliente].*

Licitud del tratamiento
La base jurídica depende del uso concreto de la herramienta de IA:
- Artículo 6.1 b) del RGPD (ejecución del contrato) si la IA se usa para prestar un servicio al interesado.
- Artículo 6.1 c) del RGPD (obligación legal) si la IA se usa para cumplir obligaciones normativas.
- Artículo 6.1 f) del RGPD (interés legítimo) para usos de productividad interna.
REGLAMENTO (UE) 2024/1689 DE IA (AI Act): verificar si los sistemas de IA utilizados son de alto riesgo (p. ej. en RRHH o acceso a servicios) y cumplir con las obligaciones específicas aplicables.
Se recomienda realizar una Evaluación de Impacto (EIPD, art. 35 RGPD) antes de implantar sistemas de IA que traten datos a gran escala o que puedan afectar significativamente a los interesados.

Plazos de conservación
El definido para la actividad de negocio subyacente. Los datos introducidos en herramientas de IA externas deben suprimirse conforme a la política del proveedor, que debe verificarse y documentarse. Política interna de uso de IA: En desarrollo.

Descripción del tratamiento	
Origen y procedencia de los datos	*Los propios usuarios de la empresa que interactúan con las herramientas de IA.*
Colectivos afectados	*Empleados, clientes o proveedores cuyos datos puedan ser introducidos en herramientas de IA.*

Categorías de datos tratados	
Tipologías de datos	
Infracciones	*n/a*
Categorías especiales de datos	*Verificar — [PENDIENTE de confirmar por el cliente].*
Datos identificativos	*Los que correspondan según el uso concreto de la herramienta.*
Otros	*Herramientas utilizadas: [PENDIENTE — completar por el cliente]. Usos: [PENDIENTE — completar por el cliente]. Estado DPA con proveedores: [PENDIENTE].*

Medidas de seguridad
Política interna de uso de IA: En desarrollo — pendiente de completar y comunicar a empleados.
Verificar y documentar las condiciones de uso de datos de cada proveedor de IA.
Restringir la introducción de datos personales sensibles en herramientas de IA sin autorización previa.
Control de acceso por usuario y contraseña con política de contraseñas corporativa.
Autenticación de doble factor (2FA) en acceso a sistemas con datos personales.
Cifrado de disco en equipos informáticos.
Antivirus y firewall activos en todos los equipos.
Copias de seguridad diaria almacenadas en servidor externo.

Copias de seguridad cifradas.

Compromisos de confidencialidad firmados por todo el personal con acceso a datos personales.

Procedimiento documentado para atender el ejercicio de derechos RGPD.

Registro de accesos a sistemas con datos personales.

⚠

Comunicaciones de datos

- Proveedor/es de herramientas de IA utilizadas: [PENDIENTE — completar por el cliente] (pueden actuar como encargado del tratamiento o como responsable independiente según sus condiciones; verificar caso a caso).

Transferencia internacional de datos

Transferencias Internacionales de datos

No están previstas