# Contrato de encargo del tratamiento

Versión 1.0, de 16 de noviembre de 2026

Anexo V de las condiciones generales del servicio Crelia.

## Partes

**El responsable del tratamiento («el cliente»):** la empresa o el profesional que contrata el servicio Crelia, con los datos que constan en su cuenta (razón social, NIF y domicilio), representado por la persona que acepta este contrato en su nombre.

**La encargada del tratamiento («Myolos»):** Myolos Consultoría y Diseño Web S.L., NIF B72594716, Rúa Cunchido de Abaixo, 44, 36940 Cangas (Pontevedra). Contacto de protección de datos: privacidad@crelia.es.

## 1. Objeto

Myolos trata, por cuenta del cliente, los datos personales necesarios para prestarle los servicios que contrata con las condiciones generales del servicio Crelia: la plataforma y, si lo contrata, el asesoramiento. Este contrato fija las condiciones de ese tratamiento.

## 2. Descripción del tratamiento

El anexo A describe a quién se refieren los datos, qué datos son, qué operaciones se hacen con ellos y para qué.

## 3. Duración

Dura lo mismo que el servicio. Las obligaciones de la cláusula 15 (fin de la prestación) y el deber de confidencialidad siguen vigentes después, mientras Myolos conserve algún dato del cliente.

## 4. Instrucciones del responsable

1. Myolos trata los datos **solo siguiendo las instrucciones documentadas del cliente**, también en lo que toca a las transferencias internacionales. Son instrucciones documentadas: este contrato, las condiciones generales y lo que el cliente hace con las funciones de la plataforma (dar de alta a personas y darles permisos, dar acceso a un asesor, generar un enlace de inspección, activar módulos, pedir una exportación o una supresión).
2. Si una ley de la Unión Europea o de España obliga a Myolos a tratar los datos de otro modo, se lo dice al cliente antes de hacerlo, salvo que esa ley lo prohíba.
3. Si Myolos cree que una instrucción infringe la normativa de protección de datos, se lo dice de inmediato al cliente.
4. Myolos **no usa los datos para fines propios**: ni análisis de uso con fines comerciales, ni publicidad, ni entrenamiento de modelos, ni cesión a terceros, ni para valorar a ninguna persona con el registro de actividad. Si lo hiciera, sería responsable de ese tratamiento (art. 28.10 del RGPD).
5. El cliente autoriza a Myolos a obtener, a partir del uso del servicio, estadísticas agregadas y anónimas (por ejemplo, cuántos documentos se crean o qué funciones se usan) que no identifican a ninguna persona ni al cliente, y a usarlas para mantener y mejorar el servicio. Una vez anonimizadas, no son datos personales ni datos del cliente.

## 5. Confidencialidad

1. Solo acceden a los datos las personas de Myolos que lo necesitan para prestar el servicio. Cada una ha firmado un compromiso de confidencialidad, que sigue vigente al terminar su relación con Myolos, y conoce las medidas de seguridad que debe aplicar.

2. Quién puede acceder y cuándo lo fija la política interna de acceso a los datos de los clientes de Myolos (anexo B).

## 6. Seguridad

1. Myolos aplica las medidas técnicas y organizativas del anexo B, apropiadas al riesgo (art. 32 del RGPD).
2. Las revisa periódicamente y puede sustituir una medida por otra siempre que no baje el nivel de protección.

## 7. Acceso de la encargada a la cuenta del cliente

1. Myolos solo consulta la cuenta del cliente para:
2. dar el **soporte que el cliente pide**, que es la instrucción para esa consulta;
3. contener o investigar un **incidente de seguridad** o una avería, sin permiso previo, avisando después al cliente;
4. atender una **exportación o una supresión** que el cliente pide;
5. cumplir una **obligación legal**, en los términos de la cláusula 4.2.
6. Cada consulta queda anotada en el registro de actividad de la cuenta, y el titular la ve.

## 8. Asesores y control oficial

1. **Asesor interno.** El técnico de Crelia que asesora al cliente es personal de Myolos: su trabajo con los datos del cliente es parte de este encargo. Accede a la cuenta solo mientras el titular se lo permite.
2. **Asesor externo.** El asesor de otra asesoría al que el cliente da acceso trata los datos por cuenta del cliente, con el contrato que el cliente tenga con él. No es subencargado de Myolos. Myolos limita su acceso a lo que permite la plataforma y anota sus consultas; el cliente le da y le retira el acceso, y debe firmar con él su propio contrato de encargo.
3. **Inspección.** Cuando el cliente genera un enlace de inspección, es el cliente quien facilita su documentación a la autoridad de control oficial, en cumplimiento de sus obligaciones. Myolos pone el medio, limita lo que se ve a la documentación aprobada que cada módulo declara para la inspección (nunca las fichas de personal) y anota cada uso del enlace.

## 9. Subencargados

1. El cliente **autoriza de forma general** a Myolos a recurrir a los subencargados del anexo D.
2. Antes de añadir o sustituir un subencargado, Myolos avisa al cliente **con 15 días de antelación**, por correo al contacto de protección de datos y en el área, con el nombre del proveedor, el servicio, la ubicación de los datos y la garantía de transferencia, si la hay. Lo mismo vale para los cambios de los subencargados de sus subencargados, en cuanto Myolos los conozca.
3. El cliente puede **oponerse** por escrito y con un motivo razonable de protección de datos dentro de ese plazo. Si Myolos no puede atender la oposición, el cliente puede darse de baja antes de que el cambio surta efecto, con la salida de la cláusula 8 de las condiciones generales.
4. Si la sustitución es urgente para mantener la seguridad o la continuidad del servicio, Myolos la hace y avisa en cuanto pueda; el cliente conserva el derecho del apartado 3.
5. Myolos impone a cada subencargado, por contrato, las mismas obligaciones de protección de datos que este contrato le impone a ella (art. 28.4 del RGPD), y responde ante el cliente de su cumplimiento.
6. Myolos tiene a disposición del cliente la lista actualizada de sus subencargados y de los subencargados de estos que tratan datos del cliente.

## 10. Transferencias internacionales

Myolos no trata ni deja tratar los datos fuera del Espacio Económico Europeo, salvo con una de las garantías de los arts. 44 a 49 del RGPD, que se indica en el anexo D y que el cliente conoce con el aviso de la cláusula 9.2.

## 11. Violaciones de la seguridad de los datos

1. Myolos avisa al cliente de toda violación de la seguridad que afecte a sus datos **sin dilación indebida y, como máximo, en 48 horas** desde que tiene constancia de ella, por correo al contacto para incidentes y, si es posible, en el área. Avisa sin esperar a valorar el riesgo, que valora el cliente.
2. El aviso incluye lo que pide el art. 33.3 del RGPD que se sepa en ese momento: qué ha pasado, a qué categorías y a cuántas personas y registros afecta aproximadamente, sus consecuencias probables, las medidas tomadas o propuestas y un contacto. Lo que no se sepa aún se da después, por fases, sin esperar a tenerlo todo.
3. Decidir si se notifica a la Agencia Española de Protección de Datos y a las personas afectadas corresponde al cliente. Myolos le **asiste**: le da la información que necesita para notificar, le propone el texto y, si el cliente se lo pide por escrito, puede enviar en su nombre la comunicación a las personas usuarias afectadas por los avisos de la plataforma.
4. Myolos documenta cada violación, sus efectos y las medidas tomadas, y entrega esa documentación al cliente si la pide.
5. El cliente comunica a Myolos cualquier incidente que conozca en privacidad@crelia.es o por los mensajes del área.

## 12. Ejercicio de derechos de los interesados

1. Si una persona pide a Myolos el ejercicio de un derecho sobre datos de la cuenta del cliente, Myolos lo traslada al cliente sin dilación indebida y, como máximo, en 2 días hábiles desde que lo recibe, por correo al contacto de protección de datos, sin responder por su cuenta salvo para decir que lo ha trasladado.
2. La plataforma permite al cliente atender por sí mismo la rectificación (desde el área) y le da medios para el acceso y la portabilidad de una persona, su supresión y la oposición o limitación. Cuando el cliente necesite algo que no pueda hacer desde el área, Myolos le asiste, a petición suya por los mensajes del área o en privacidad@crelia.es, con la antelación necesaria para que pueda responder dentro del plazo legal.
3. Las entregas de datos se hacen por un canal cifrado, a quien se haya comprobado que tiene derecho a recibirlas, con la huella del fichero.

## 13. Evaluaciones de impacto y consulta previa

Myolos da al cliente la información que necesite para hacer una evaluación de impacto o una consulta previa (arts. 35 y 36 del RGPD) sobre el tratamiento en la plataforma, en la medida en que disponga de ella.

## 14. Plazos de conservación

1. Los plazos del anexo C son **instrucción del cliente** al aceptar este contrato. Son iguales para todas las cuentas.
2. El cliente puede pedir otros plazos. Si la plataforma no puede aplicarlos, Myolos se lo dice y le ofrece una alternativa (por ejemplo, la exportación y la supresión anticipada de lo que quiera).

## 15. Fin de la prestación: devolución y supresión

1. **Periodo de salida.** Cuando el cliente pide terminar el servicio, el servicio sigue con normalidad durante el **periodo transitorio de 30 días** de la cláusula 8 de las condiciones generales, que el cliente puede prorrogar una vez. Después, la cuenta pasa a baja, en solo lectura, durante un **periodo de recuperación de al menos 30 días** en que el cliente aún puede obtener sus datos. El cliente puede renunciar a los dos periodos si no los necesita.
2. **Devolución.** El titular puede descargar la exportación completa de la cuenta (anexo IV de las condiciones generales) desde el área, sin coste, durante el contrato y el periodo de salida. Si no puede hacerlo, Myolos se la entrega por un canal cifrado, con la huella del fichero, en un plazo razonable y, si la pide al terminar el contrato, dentro del periodo de salida.
3. **Supresión.** Al terminar el periodo de recuperación, Myolos suprime todos los datos de la cuenta, salvo lo

que conserva bloqueado según el apartado 5. Si el cliente lo pide, antes los entrega al nuevo proveedor que designe, en el formato de la exportación. Myolos no conserva la documentación del cliente después de la baja: es el cliente quien la conserva, con su exportación, durante los plazos que le exija la normativa. Antes de suprimir, Myolos comprueba que el cliente ha obtenido la exportación y, si no lo ha hecho, se la entrega por un canal cifrado (art. 33.3 de la Ley Orgánica 3/2018).

4. **Copias de seguridad.** Los datos suprimidos siguen en las copias de seguridad cifradas hasta que caducan (como máximo, 12 meses). No se usan ni se consultan; si hubiera que restaurar una copia, Myolos vuelve a aplicar las supresiones antes de reanudar el servicio.
5. **Bloqueo por responsabilidades.** Myolos puede conservar bloqueados, y solo para defenderse de reclamaciones derivadas de este encargo, el registro de actividad de la cuenta, los datos de acceso de sus usuarios y los registros de aceptación, mientras puedan exigirse esas responsabilidades (art. 33.4 de la Ley Orgánica 3/2018).
6. **Certificado.** Si el cliente lo pide, Myolos le entrega, al completar la supresión, un certificado que dice qué se suprimió y cuándo, qué se conserva y hasta cuándo, y hasta cuándo siguen los datos en las copias.
7. **Si Myolos deja de prestar el servicio**, devuelve los datos al cliente y los suprime, salvo que el contrato se ceda a quien continúe el servicio, como prevén las condiciones generales.

## 16. Información y auditorías

1. Myolos pone a disposición del cliente, si la pide, la información necesaria para demostrar que cumple este contrato.
2. Si esa información no basta, el cliente, o un auditor que designe obligado a confidencialidad y que no sea competidor de Myolos, puede auditar el cumplimiento con 30 días de preaviso, con el alcance acordado antes, en horario laborable y una vez al año como máximo, salvo tras una violación de seguridad o a petición de una autoridad. La auditoría no da acceso a datos de otros clientes ni a la seguridad de la plataforma más allá de lo necesario. Su coste, incluido el tiempo de Myolos, es del cliente, salvo que revele un incumplimiento grave de Myolos.

## 17. Obligaciones del responsable

1. Tener una base jurídica para los datos que guarda en la plataforma e informar a las personas, en particular a su personal (Myolos le ofrece un modelo).
2. No guardar categorías especiales de datos (por ejemplo, de salud) salvo que sean imprescindibles y lícitas, y nunca en campos que no estén pensados para ellas.
3. Designar un contacto de protección de datos y para incidentes, distinto del correo de la cuenta, y mantenerlo al día.
4. Dar y retirar con diligencia el acceso de sus personas, de los asesores y de los enlaces de inspección.
5. Firmar su propio contrato de encargo con el asesor externo al que dé acceso.
6. Supervisar el tratamiento, incluidas las auditorías de la cláusula 16.

## 18. Responsabilidad

Frente a las personas afectadas y a las autoridades, cada parte responde según los arts. 82 y 83 del RGPD. Entre las partes, cada una responde de los daños que cause a la otra por incumplir este contrato o la normativa de protección de datos, con los límites de la cláusula 14 de las condiciones generales, que no se aplican en caso de dolo o culpa grave.

## 19. Prelación, modificación y ley aplicable

1. En lo que toca a la protección de datos, este contrato prevalece sobre las condiciones generales.
2. Se modifica por el procedimiento de la cláusula 16 de las condiciones generales. Los cambios de los anexos B y D siguen las cláusulas 6.2 y 9.
3. Se rige por la ley española, y las controversias se resuelven como dice la cláusula 20 de las condiciones

generales.

*Última actualización: 16 de noviembre de 2026. Versión 1.0.*

---

## Anexo A. Descripción del tratamiento

| Elemento | Descripción |
|---|---|
| **Personas a las que se refieren los datos** | Personal del cliente y de sus locales (empleados, encargados, coadministradores, el titular como persona usuaria); personas que figuran en las fichas de personal; el cliente si es persona física; personas de contacto de proveedores y servicios externos del local; asesores en lo que hacen dentro de la cuenta; quien abre un enlace de inspección |
| **Datos** | Identificativos y de contacto profesional (nombre, puesto, teléfono y correo del trabajo); nombre de usuario, contraseña cifrada y métodos de segundo factor; papel, locales y permisos; responsabilidades que ocupa cada persona y sus fechas; fechas en que una persona no está disponible para el trabajo, **sin el motivo**; autoría y fecha de cada registro (quién aprobó, revisó, imprimió o cambió); consultas y descargas; mensajes, propuestas y revisiones; avisos; datos de la empresa y del local (si el cliente es persona física, son datos personales); huella cifrada del origen de cada petición y de cada uso del enlace de inspección |
| **Categorías especiales** | No se prevén. La plataforma no tiene campos de salud ni de otras categorías especiales. Los textos libres y ficheros podrían contenerlas: el uso aceptable lo prohíbe salvo que sean imprescindibles y lícitas |
| **Operaciones** | Recogida, registro, organización, conservación, consulta, modificación, comunicación al asesor y a la autoridad por decisión del cliente, exportación, seudonimización, anonimización para estadísticas de uso, bloqueo y supresión |
| **Finalidad** | Prestar al cliente la plataforma y el asesoramiento: custodiar su documentación de seguridad alimentaria, ayudarle a mantenerla, colaborar con su asesor, facilitarla a la inspección y devolvérsela al final |
| **Duración** | La del servicio y la de la cláusula 15 |
| **Dónde** | En los servidores del anexo D, en el Espacio Económico Europeo [confirmar], y en el navegador de cada persona usuaria (copias temporales que no salen de su dispositivo) |

## Anexo B. Medidas técnicas y organizativas

Medidas comprobadas en el programa. Las marcadas **[alojamiento]** dependen del proveedor y se completan antes del primer cliente.

### Separación entre clientes

- Cada dato lleva la cuenta a la que pertenece y la base de datos filtra por cuenta en cada lectura y en cada escritura (seguridad por filas), también frente al propietario de las tablas. La cuenta de cada petición la fija el servidor, firmada; no se toma de lo que envía el navegador.
- Las pruebas de acceso cruzado entre cuentas se repiten en cada versión.
- Las tablas del gestor de contenidos para sesiones, usuarios y segundo factor no tienen esa separación; lo compensan una regla del código que rechaza las consultas que concatenan texto, pruebas de inyección en cada versión y una revisión anual.
- La vía técnica que salta la separación entre cuentas solo la usan las tareas automáticas y las acciones de administración previstas, según la política interna de acceso.

### Identidad y acceso

- Segundo factor obligatorio para titulares, coadministradores, asesores y administración.
- La sesión se cierra tras 30 minutos sin actividad.
- Límite de intentos de entrada por usuario y por origen, con bloqueo temporal y aviso al titular; la respuesta

a un rechazo no revela si el usuario existe.
- Alta solo por invitación y en cadena; ninguna cuenta de cliente entra en la administración.
- Permisos por papel y por local, denegados por defecto; permisos puntuales con duración.
- Los enlaces de un solo uso caducan a las 24 horas; de los enlaces solo se guarda una huella.

### Integridad y trazabilidad

- Cada escritura queda atribuida a su autor, con la hora del servidor, en un registro que la base de datos no deja modificar ni borrar.
- Los documentos aprobados no se cambian: corregirlos crea una versión nueva. Las conversaciones, las revisiones cerradas y las propuestas decididas no se editan ni se borran.
- Las consultas y descargas del asesor y del soporte quedan anotadas y el titular las ve.

### Confidencialidad

- Conexión cifrada obligatoria, cabeceras de seguridad y ningún recurso cargado de servidores de terceros.
- Los ficheros se guardan fuera de la parte pública del servidor, se comprueba su tipo real y solo se descargan con permiso.
- El registro de errores no guarda los valores que contiene un error.
- La clave con que se firman las peticiones y se calculan las huellas es propia de producción y no se copia de otros entornos.
- Cifrado de la base de datos y de los ficheros guardados **[alojamiento]**.

### Disponibilidad y copias

- Copia diaria, cifrada y fuera del servidor principal; se guardan 30 diarias y 12 mensuales **[proveedor de copias]**.
- Plan escrito de recuperación; pérdida máxima de datos y tiempo máximo de recuperación de 24 horas cada uno, que pasan a 1 hora y 4 horas cuando la plataforma gestione los lotes de producción o llegue a 20 cuentas de pago.
- Prueba de restauración en el alojamiento definitivo antes del primer cliente y después periódicamente **[alojamiento]**.
- Las supresiones se vuelven a aplicar tras restaurar una copia **[mecanismo por implantar]**.

### Organización

- Compromiso de confidencialidad firmado por cada persona con acceso.
- Política interna de acceso a los datos de los clientes, con revisión periódica de los accesos.
- Procedimientos escritos de incidentes de seguridad, de solicitudes de derechos y de exportación, y de recuperación, con simulacros periódicos.
- Contratos de encargo con cada subencargado y comprobación previa de sus garantías.

## Anexo C. Plazos de conservación

**Durante el servicio.** El cliente mantiene, corrige y borra sus datos desde el área. La plataforma aplica, además, estos plazos:

| Datos | Plazo |
|---|---|
| Registro de actividad | Lo que documenta un registro, mientras exista ese registro; las consultas, accesos y denegaciones, 2 años |
| Intentos de entrada (su anotación) | 12 meses, y después se seudonimiza |
| Uso de los enlaces de inspección | Lo mismo que el registro de actividad |

**Al terminar el servicio.** Al terminar el periodo de recuperación, todos los datos de la cuenta se suprimen (cláusula 15.3), salvo lo que se conserva bloqueado según la cláusula 15.5:

| Datos | Plazo del bloqueo |
|---|---|
| Registro de actividad de la cuenta | 5 años; después se seudonimiza |
| Datos de acceso de los usuarios | 3 años; después se anonimizan |
| Registros de aceptación | 6 años |

## Anexo D. Subencargados autorizados

| Subencargado | Servicio | Ubicación de los datos | Garantía de transferencia |
|---|---|---|---|
| [pendiente] | Alojamiento del sitio y de la base de datos | [pendiente] | [no aplica si está en el EEE] |
| [pendiente] | Correo de salida | [pendiente] | [pendiente] |
| [pendiente] | Copias de seguridad | [pendiente] | [pendiente] |