Contrato de encargo do tratamento

Versión 1.0, do 16 de novembro de 2026

Este texto ofrécese en castelán e en galego. En caso de discrepancia entre as dúas versións, prevalece a castelá.

Anexo V das condicións xerais do servizo Crelia.

Partes

O responsable do tratamento («o cliente»): a empresa ou o profesional que contrata o servizo Crelia, cos datos que constan na súa conta (razón social, NIF e domicilio), representado pola persoa que acepta este contrato no seu nome.

A encargada do tratamento («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. Obxecto

Myolos trata, por conta do cliente, os datos persoais necesarios para prestarlle os servizos que contrata coas condicións xerais do servizo Crelia: a plataforma e, se o contrata, o asesoramento. Este contrato fixa as condicións dese tratamento.

2. Descrición do tratamento

O anexo A describe a quen se refiren os datos, que datos son, que operacións se fan con eles e para que.

3. Duración

Dura o mesmo que o servizo. As obrigas da cláusula 15 (fin da prestación) e o deber de confidencialidade seguen vixentes despois, mentres Myolos conserve algún dato do cliente.

4. Instrucións do responsable

1. Myolos trata os datos **só seguindo as instrucións documentadas do cliente**, tamén no que toca ás transferencias internacionais. Son instrucións documentadas: este contrato, as condicións xerais e o que o cliente fai coas funcións da plataforma (dar de alta persoas e darlles permisos, dar acceso a un asesor, xerar unha ligazón de inspección, activar módulos, pedir unha exportación ou unha supresión).
2. Se unha lei da Unión Europea ou de España obriga Myolos a tratar os datos doutro xeito, dillo ao cliente antes de facelo, salvo que esa lei o prohíba.
3. Se Myolos cre que unha instrución infrinxe a normativa de protección de datos, dillo de inmediato ao cliente.
4. Myolos **non usa os datos para fins propios**: nin análise de uso con fins comerciais, nin publicidade, nin adestramento de modelos, nin cesión a terceiros, nin para valorar ningunha persoa co rexistro de actividade. Se o fixese, sería responsable dese tratamento (art. 28.10 do RGPD).
5. O cliente autoriza Myolos a obter, a partir do uso do servizo, estatísticas agregadas e anónimas (por exemplo, cantos documentos se crean ou que funcións se usan) que non identifican ningunha persoa nin o cliente, e a usalas para manter e mellorar o servizo. Unha vez anonimizadas, non son datos persoais nin datos do cliente.

5. Confidencialidade

1. Só acceden aos datos as persoas de Myolos que o necesitan para prestar o servizo. Cada unha asinou un compromiso de confidencialidade, que segue vixente ao rematar a súa relación con Myolos, e coñece as medidas de seguridade que debe aplicar.

2. Quen pode acceder e cando o fixa a política interna de acceso aos datos dos clientes de Myolos (anexo B).

6. Seguridade

1. Myolos aplica as medidas técnicas e organizativas do anexo B, apropiadas ao risco (art. 32 do RGPD).
2. Revísaas periodicamente e pode substituír unha medida por outra sempre que non baixe o nivel de protección.

7. Acceso da encargada á conta do cliente

1. Myolos só consulta a conta do cliente para:
2. dar o **soporte que o cliente pide**, que é a instrución para esa consulta;
3. conter ou investigar un **incidente de seguridade** ou unha avaría, sen permiso previo, avisando despois o cliente;
4. atender unha **exportación ou unha supresión** que o cliente pide;
5. cumprir unha **obriga legal**, nos termos da cláusula 4.2.
6. Cada consulta queda anotada no rexistro de actividade da conta, e o titular vea.

8. Asesores e control oficial

1. **Asesor interno.** O técnico de Crelia que asesora o cliente é persoal de Myolos: o seu traballo cos datos do cliente é parte deste encargo. Accede á conta só mentres o titular llo permite.
2. **Asesor externo.** O asesor doutra asesoría ao que o cliente dá acceso trata os datos por conta do cliente, co contrato que o cliente teña con el. Non é subencargado de Myolos. Myolos limita o seu acceso ao que permite a plataforma e anota as súas consultas; o cliente dálle e retíralle o acceso, e debe asinar con el o seu propio contrato de encargo.
3. **Inspección.** Cando o cliente xera unha ligazón de inspección, é o cliente quen facilita a súa documentación á autoridade de control oficial, en cumprimento das súas obrigas. Myolos pon o medio, limita o que se ve á documentación aprobada que cada módulo declara para a inspección (nunca as fichas de persoal) e anota cada uso da ligazón.

9. Subencargados

1. O cliente **autoriza de forma xeral** Myolos a recorrer aos subencargados do anexo D.
2. Antes de engadir ou substituír un subencargado, Myolos avisa o cliente **con 15 días de antelación**, por correo ao contacto de protección de datos e na área, co nome do provedor, o servizo, a ubicación dos datos e a garantía de transferencia, se a hai. O mesmo vale para os cambios dos subencargados dos seus subencargados, en canto Myolos os coñeza.
3. O cliente pode **opoñerse** por escrito e cun motivo razoable de protección de datos dentro dese prazo. Se Myolos non pode atender a oposición, o cliente pode darse de baixa antes de que o cambio surta efecto, coa saída da cláusula 8 das condicións xerais.
4. Se a substitución é urxente para manter a seguridade ou a continuidade do servizo, Myolos faina e avisa en canto poida; o cliente conserva o dereito do apartado 3.
5. Myolos impón a cada subencargado, por contrato, as mesmas obrigas de protección de datos que este contrato lle impón a ela (art. 28.4 do RGPD), e responde ante o cliente do seu cumprimento.
6. Myolos ten á disposición do cliente a lista actualizada dos seus subencargados e dos subencargados destes que tratan datos do cliente.

10. Transferencias internacionais

Myolos non trata nin deixa tratar os datos fóra do Espazo Económico Europeo, salvo cunha das garantías dos arts. 44 a 49 do RGPD, que se indica no anexo D e que o cliente coñece co aviso da cláusula 9.2.

11. Violacións da seguridade dos datos

1. Myolos avisa o cliente de toda violación da seguridade que afecte os seus datos **sen dilación indebida e, como máximo, en 48 horas** desde que ten constancia dela, por correo ao contacto para incidentes e, se é posible, na área. Avisa sen esperar a valorar o risco, que valora o cliente.
2. O aviso inclúe o que pide o art. 33.3 do RGPD que se saiba nese momento: que pasou, a que categorías e a cantas persoas e rexistros afecta aproximadamente, as súas consecuencias probables, as medidas tomadas ou propostas e un contacto. O que aínda non se saiba dáse despois, por fases, sen esperar a telo todo.
3. Decidir se se notifica á Axencia Española de Protección de Datos e ás persoas afectadas corresponde ao cliente. Myolos **asísteo**: dálle a información que necesita para notificar, proponlle o texto e, se o cliente llo pide por escrito, pode enviar no seu nome a comunicación ás persoas usuarias afectadas polos avisos da plataforma.
4. Myolos documenta cada violación, os seus efectos e as medidas tomadas, e entrega esa documentación ao cliente se a pide.
5. O cliente comunica a Myolos calquera incidente que coñeza en privacidad@crelia.es ou polas mensaxes da área.

12. Exercicio de dereitos das persoas interesadas

1. Se unha persoa pide a Myolos o exercicio dun dereito sobre datos da conta do cliente, Myolos trasládao ao cliente sen dilación indebida e, como máximo, en 2 días hábiles desde que o recibe, por correo ao contacto de protección de datos, sen responder pola súa conta salvo para dicir que o trasladou.
2. A plataforma permite ao cliente atender por si mesmo a rectificación (desde a área) e dálle medios para o acceso e a portabilidade dunha persoa, a súa supresión e a oposición ou limitación. Cando o cliente necesite algo que non poida facer desde a área, Myolos asísteo, a petición del polas mensaxes da área ou en privacidad@crelia.es, coa antelación necesaria para que poida responder dentro do prazo legal.
3. As entregas de datos fanse por unha canle cifrada, a quen se comprobase que ten dereito a recibilas, coa pegada do ficheiro.

13. Avaliacións de impacto e consulta previa

Myolos dá ao cliente a información que necesite para facer unha avaliación de impacto ou unha consulta previa (arts. 35 e 36 do RGPD) sobre o tratamento na plataforma, na medida en que dispoña dela.

14. Prazos de conservación

1. Os prazos do anexo C son **instrución do cliente** ao aceptar este contrato. Son iguais para todas as contas.
2. O cliente pode pedir outros prazos. Se a plataforma non pode aplicalos, Myolos dillo e ofrécelle unha alternativa (por exemplo, a exportación e a supresión anticipada do que queira).

15. Fin da prestación: devolución e supresión

1. **Período de saída.** Cando o cliente pide rematar o servizo, o servizo segue con normalidade durante o **período transitorio de 30 días** da cláusula 8 das condicións xerais, que o cliente pode prorrogar unha vez. Despois, a conta pasa a baixa, en só lectura, durante un **período de recuperación de polo menos 30 días** en que o cliente aínda pode obter os seus datos. O cliente pode renunciar aos dous períodos se non os necesita.
2. **Devolución.** O titular pode descargar a exportación completa da conta (anexo IV das condicións xerais) desde a área, sen custo, durante o contrato e o período de saída. Se non pode facelo, Myolos entrégalla por unha canle cifrada, coa pegada do ficheiro, nun prazo razoable e, se a pide ao rematar o contrato, dentro do período de saída.
3. **Supresión.** Ao rematar o período de recuperación, Myolos suprime todos os datos da conta, salvo o que

conserva bloqueado segundo o apartado 5. Se o cliente o pide, entrégaos antes ao novo provedor que designe, no formato da exportación. Myolos non conserva a documentación do cliente despois da baixa: é o cliente quen a conserva, coa súa exportación, durante os prazos que lle esixa a normativa. Antes de suprimir, Myolos comproba que o cliente obtivo a exportación e, se non o fixo, entrégalla por unha canle cifrada (art. 33.3 da Lei orgánica 3/2018).

4. **Copias de seguridade.** Os datos suprimidos seguen nas copias de seguridade cifradas ata que caducan (como máximo, 12 meses). Non se usan nin se consultan; se houbese que restaurar unha copia, Myolos volve aplicar as supresións antes de retomar o servizo.
5. **Bloqueo por responsabilidades.** Myolos pode conservar bloqueados, e só para defenderse de reclamacións derivadas deste encargo, o rexistro de actividade da conta, os datos de acceso dos seus usuarios e os rexistros de aceptación, mentres se poidan esixir esas responsabilidades (art. 33.4 da Lei orgánica 3/2018).
6. **Certificado.** Se o cliente o pide, Myolos entrégalle, ao completar a supresión, un certificado que di o que se suprimiu e cando, o que se conserva e ata cando, e ata cando seguen os datos nas copias.
7. **Se Myolos deixa de prestar o servizo**, devolve os datos ao cliente e suprímeos, salvo que o contrato se ceda a quen continúe o servizo, como prevén as condicións xerais.

16. Información e auditorías

1. Myolos pon á disposición do cliente, se a pide, a información necesaria para demostrar que cumpre este contrato.
2. Se esa información non abonda, o cliente, ou un auditor que designe obrigado a confidencialidade e que non sexa competidor de Myolos, pode auditar o cumprimento con 30 días de preaviso, co alcance acordado antes, en horario laborable e unha vez ao ano como máximo, salvo tras unha violación de seguridade ou a petición dunha autoridade. A auditoría non dá acceso a datos doutros clientes nin á seguridade da plataforma máis alá do necesario. O seu custo, incluído o tempo de Myolos, é do cliente, salvo que revele un incumprimento grave de Myolos.

17. Obrigas do responsable

1. Ter unha base xurídica para os datos que garda na plataforma e informar as persoas, en particular o seu persoal (Myolos ofrécelle un modelo).
2. Non gardar categorías especiais de datos (por exemplo, de saúde) salvo que sexan imprescindibles e lícitas, e nunca en campos que non estean pensados para elas.
3. Designar un contacto de protección de datos e para incidentes, distinto do correo da conta, e mantelo ao día.
4. Dar e retirar con dilixencia o acceso das súas persoas, dos asesores e das ligazóns de inspección.
5. Asinar o seu propio contrato de encargo co asesor externo ao que dea acceso.
6. Supervisar o tratamento, incluídas as auditorías da cláusula 16.

18. Responsabilidade

Fronte ás persoas afectadas e ás autoridades, cada parte responde segundo os arts. 82 e 83 do RGPD. Entre as partes, cada unha responde dos danos que cause á outra por incumprir este contrato ou a normativa de protección de datos, cos límites da cláusula 14 das condicións xerais, que non se aplican en caso de dolo ou culpa grave.

19. Prelación, modificación e lei aplicable

1. No que toca á protección de datos, este contrato prevalece sobre as condicións xerais.
2. Modifícase polo procedemento da cláusula 16 das condicións xerais. Os cambios dos anexos B e D seguen as cláusulas 6.2 e 9.
3. Réxese pola lei española, e as controversias resólvense como di a cláusula 20 das condicións xerais.

Última actualización: 16 de novembro de 2026. Versión 1.0.

Anexo A. Descrición do tratamento

Elemento	Descrición
Persoas ás que se refiren os datos	Persoal do cliente e dos seus locais (empregados, encargados, coadministradores, o titular como persoa usuaria); persoas que figuran nas fichas de persoal; o cliente se é persoa física; persoas de contacto de provedores e servizos externos do local; asesores no que fan dentro da conta; quen abre unha ligazón de inspección
Datos	Identificativos e de contacto profesional (nome, posto, teléfono e correo do traballo); nome de usuario, contrasinal cifrado e métodos de segundo factor; papel, locais e permisos; responsabilidades que ocupa cada persoa e as súas datas; datas en que unha persoa non está dispoñible para o traballo, **sen o motivo**; autoría e data de cada rexistro (quen aprobou, revisou, imprimiu ou cambiou); consultas e descargas; mensaxes, propostas e revisións; avisos; datos da empresa e do local (se o cliente é persoa física, son datos persoais); pegada cifrada da orixe de cada petición e de cada uso da ligazón de inspección
Categorías especiais	Non se prevén. A plataforma non ten campos de saúde nin doutras categorías especiais. Os textos libres e ficheiros poderían contelas: o uso aceptable prohíbeo salvo que sexan imprescindibles e lícitas
Operacións	Recollida, rexistro, organización, conservación, consulta, modificación, comunicación ao asesor e á autoridade por decisión do cliente, exportación, pseudonimización, anonimización para estatísticas de uso, bloqueo e supresión
Finalidade	Prestar ao cliente a plataforma e o asesoramento: custodiar a súa documentación de seguridade alimentaria, axudalo a mantela, colaborar co seu asesor, facilitala á inspección e devolverlla ao final
Duración	A do servizo e a da cláusula 15
Onde	Nos servidores do anexo D, no Espazo Económico Europeo [confirmar], e no navegador de cada persoa usuaria (copias temporais que non saen do seu dispositivo)

Anexo B. Medidas técnicas e organizativas

Medidas comprobadas no programa. As marcadas **[aloxamento]** dependen do provedor e complétanse antes do primeiro cliente.

Separación entre clientes

- Cada dato leva a conta á que pertence e a base de datos filtra por conta en cada lectura e en cada escritura (seguridade por filas), tamén fronte ao propietario das táboas. A conta de cada petición fíxaa o servidor, asinada; non se toma do que envía o navegador.
- As probas de acceso cruzado entre contas repítense en cada versión.
- As táboas do xestor de contidos para sesións, usuarios e segundo factor non teñen esa separación; compénsano unha regra do código que rexeita as consultas que concatenan texto, probas de inxección en cada versión e unha revisión anual.
- A vía técnica que salta a separación entre contas só a usan as tarefas automáticas e as accións de administración previstas, segundo a política interna de acceso.

Identidade e acceso

- Segundo factor obrigatorio para titulares, coadministradores, asesores e administración.
- A sesión péchase tras 30 minutos sen actividade.
- Límite de intentos de entrada por usuario e por orixe, con bloqueo temporal e aviso ao titular; a resposta a un rexeitamento non revela se o usuario existe.
- Alta só por invitación e en cadea; ningunha conta de cliente entra na administración.
- Permisos por papel e por local, denegados por defecto; permisos puntuais con duración.

- As ligazóns dun só uso caducan ás 24 horas; das ligazóns só se garda unha pegada.

Integridade e trazabilidade

- Cada escritura queda atribuída ao seu autor, coa hora do servidor, nun rexistro que a base de datos non deixa modificar nin borrar.
- Os documentos aprobados non se cambian: corrixilos crea unha versión nova. As conversas, as revisións pechadas e as propostas decididas non se editan nin se borran.
- As consultas e descargas do asesor e do soporte quedan anotadas e o titular veas.

Confidencialidade

- Conexión cifrada obrigatoria, cabeceiras de seguridade e ningún recurso cargado de servidores de terceiros.
- Os ficheiros gárdanse fóra da parte pública do servidor, compróbase o seu tipo real e só se descargan con permiso.
- O rexistro de erros non garda os valores que contén un erro.
- A clave con que se asinan as peticións e se calculan as pegadas é propia de produción e non se copia doutros contornos.
- Cifrado da base de datos e dos ficheiros gardados **[aloxamento]**.

Dispoñibilidade e copias

- Copia diaria, cifrada e fóra do servidor principal; gárdanse 30 diarias e 12 mensuais **[provedor de copias]**.
- Plan escrito de recuperación; perda máxima de datos e tempo máximo de recuperación de 24 horas cada un, que pasan a 1 hora e 4 horas cando a plataforma xestione os lotes de produción ou chegue a 20 contas de pagamento.
- Proba de restauración no aloxamento definitivo antes do primeiro cliente e despois periodicamente **[aloxamento]**.
- As supresións vólvense aplicar tras restaurar unha copia **[mecanismo por implantar]**.

Organización

- Compromiso de confidencialidade asinado por cada persoa con acceso.
- Política interna de acceso aos datos dos clientes, con revisión periódica dos accesos.
- Procedementos escritos de incidentes de seguridade, de solicitudes de dereitos e de exportación, e de recuperación, con simulacros periódicos.
- Contratos de encargo con cada subencargado e comprobación previa das súas garantías.

Anexo C. Prazos de conservación

Durante o servizo. O cliente mantén, corrixe e borra os seus datos desde a área. A plataforma aplica, ademais, estes prazos:

Datos	Prazo
Rexistro de actividade	O que documenta un rexistro, mentres exista ese rexistro; as consultas, accesos e denegacións, 2 anos
Intentos de entrada (a súa anotación)	12 meses, e despois pseudonimízase
Uso das ligazóns de inspección	O mesmo que o rexistro de actividade

Ao rematar o servizo. Ao rematar o período de recuperación, todos os datos da conta suprímense (cláusula 15.3), salvo o que se conserva bloqueado segundo a cláusula 15.5:

Datos	Prazo do bloqueo
Rexistro de actividade da conta	5 anos; despois pseudonimízase
Datos de acceso dos usuarios	3 anos; despois anonimízanse
Rexistros de aceptación	6 anos

Anexo D. Subencargados autorizados

Subencargado	Servizo	Ubicación dos datos	Garantía de transferencia
[pendente]	Aloxamento do sitio e da base de datos	[pendente]	[non se aplica se está no EEE]
[pendente]	Correo de saída	[pendente]	[pendente]
[pendente]	Copias de seguridade	[pendente]	[pendente]