Acuerdo de Tratamiento de Datos

Versión 3.0 · 3 de septiembre de 2026 · MIND2 CREATIONS, S.L., NIF B76114545, c/ Sol 21, 35500 Arrecife de Lanzarote (Las Palmas).

El Cliente y el Responsable del Tratamiento son la persona física o jurídica identificada como tal en la correspondiente Confirmación de Contratación, que forma parte inseparable de este Acuerdo.

(conforme a lo previsto en el art. 28 RGPD)

REUNIDOS

De una parte, MIND2 CREATIONS, S.L., con NIF B76114545, domicilio social en c/ Sol, 21, 35500 Arrecife de Lanzarote, Las Palmas, inscrita en el Registro Mercantil de Las Palmas, Tomo 433, Folio 31, Sección 8, Hoja IL-10.283, y dirección de contacto admin@mind2creations.com, titular y prestadora del servicio Fichajet, en adelante, MIND2 o el Encargado del Tratamiento.

Y, de otra parte, la persona física o jurídica identificada como cliente en la correspondiente Confirmación de Contratación, en adelante, el Cliente o el Responsable del Tratamiento.

MIND2 y el Cliente podrán denominarse conjuntamente como las Partes o de forma individual, cada una de ellas, como la Parte.

EXPONEN

I. Que MIND2 presta el servicio denominado Fichajet, consistente en una aplicación web de control horario y registro de jornada en modalidad de software como servicio – SaaS- cuyas funcionalidades dependen del Plan contratado y de la configuración realizada por el Cliente.

II. Que la utilización de Fichajet puede requerir que MIND2 acceda y trate datos personales por cuenta del Cliente, especialmente datos de sus personas trabajadoras, colaboradores y Usuarios Autorizados.

III. Que, respecto de dichos tratamientos, el Cliente determina los fines y los medios esenciales y actúa, con carácter general, como Responsable del Tratamiento, mientras que MIND2 actúa como Encargado del Tratamiento.

IV. Que las Partes desean regular el acceso y tratamiento de datos personales conforme al artículo 28 del Reglamento (UE) 2016/679 —RGPD—, a la Ley Orgánica 3/2018 —LOPDGDD— y a las demás normas aplicables. En consecuencia, las Partes acuerdan las siguientes:

ESTIPULACIONES

1. Integración en la relación contractual

El presente Acuerdo forma parte integrante de las Condiciones de Contratación de Fichajet y de la Confirmación de Contratación aceptadas por el Cliente.

El Acuerdo entrará en vigor en la fecha en que el Cliente acepte electrónicamente la contratación de Fichajet o en la fecha en que MIND2 comience a tratar datos personales por cuenta del Cliente, si esta fuera anterior.

En caso de contradicción entre este Acuerdo y cualquier otro documento contractual, prevalecerá este Acuerdo en todo lo relativo al tratamiento de datos personales realizado por MIND2 por cuenta del Cliente.

La descripción concreta del tratamiento se recoge en el Anexo I; las medidas técnicas y organizativas, en el Anexo II; y los subencargados autorizados, en el Anexo III.

2. Funciones de las Partes

El Cliente actúa como Responsable del Tratamiento respecto de los datos personales incorporados, generados, consultados o gestionados mediante su Cuenta de Fichajet.

MIND2 actúa como Encargado del Tratamiento respecto de dichos datos y únicamente podrá tratarlos para prestar, mantener, proteger y dar soporte al Servicio, de conformidad con las instrucciones documentadas del Cliente y con este Acuerdo.

Cuando el Cliente actúe a su vez como encargado del tratamiento por cuenta de un tercero, MIND2 tendrá la condición de subencargado. En ese supuesto, el Cliente declara que:

a) cuenta con autorización suficiente del responsable originario para contratar a MIND2;

b) está facultado para transmitir a MIND2 las instrucciones necesarias;

c) las instrucciones comunicadas son compatibles con las recibidas del responsable originario; y

d) informará a MIND2 de cualquier condición adicional que resulte aplicable.

Este Acuerdo no regula aquellos tratamientos respecto de los cuales MIND2 actúe como responsable independiente, en particular los estrictamente necesarios para gestionar la contratación, facturación, cobros, comunicaciones contractuales, cumplimiento de obligaciones legales y tratamiento de datos de representantes y personas de contacto. Esos tratamientos se regirán por la Política de Privacidad de MIND2.

MIND2 no utilizará los datos tratados por cuenta del Cliente para finalidades propias incompatibles. Si determinase por sí misma fines o medios esenciales distintos de los instruidos, tendrá la consideración de responsable respecto de ese tratamiento, sin perjuicio de las responsabilidades que procedan.

3. Objeto, naturaleza, finalidad y duración

3.1. Objeto

El objeto del encargo es la realización de las operaciones de tratamiento estrictamente necesarias para prestar los servicios de Fichajet conforme al Plan contratado y a la configuración seleccionada por el Cliente.

3.2. Naturaleza

La naturaleza del tratamiento es principalmente automatizada y comprende, según las funcionalidades habilitadas:

a) recogida y registro;

b) organización, estructuración y clasificación;

c) alojamiento, almacenamiento y conservación;

d) consulta, recuperación y puesta a disposición de Usuarios Autorizados;

e) modificación y rectificación;

f) generación de informes y registros;

g) exportación, transmisión o entrega conforme a las instrucciones del Cliente;

h) realización de copias de seguridad y restauración;

i) soporte, diagnóstico y resolución de incidencias;

j) aplicación de medidas de seguridad, registro de auditoría y control de accesos; y

k) supresión, bloqueo o devolución.

l) autenticación y gestión de accesos mediante mecanismos SSO (Single Sign-On) o sistemas equivalentes, cuando esta funcionalidad haya sido habilitada por el Cliente.

3.3. Finalidades

Las finalidades del tratamiento son:

a) gestionar el registro de inicio y finalización de jornada;

b) gestionar horarios, turnos, calendarios, libranzas, permisos, vacaciones y ausencias;

c) gestionar Usuarios Autorizados y permisos de acceso;

d) permitir la geolocalización puntual vinculada al acto de fichaje, cuando el Cliente la habilite;

e) almacenar documentos aportados por el Cliente cuando la funcionalidad forme parte del plan contratado;

f) generar, consultar y exportar registros, informes y documentos;

g) prestar soporte técnico y resolver incidencias;

h) garantizar la seguridad, integridad, disponibilidad y continuidad del Servicio; y

i) ejecutar las demás funcionalidades contratadas y lícitamente configuradas por el Cliente.

j) permitir la autenticación de Usuarios Autorizados y, cuando proceda, la realización de operaciones de fichaje mediante integración con aplicaciones o sistemas del Cliente utilizando mecanismos SSO.

3.4. Duración

El tratamiento se mantendrá durante la vigencia de la contratación y, tras su terminación, durante los periodos de transición, recuperación, devolución, supresión y rotación de copias de seguridad previstos en este Acuerdo.

4. Instrucciones documentadas

MIND2 tratará los datos responsabilidad del Cliente siguiendo instrucciones documentadas del Cliente. Tendrán la consideración de instrucciones documentadas del Cliente:

a) el presente Acuerdo;

b) las Condiciones de Contratación y la Confirmación de Contratación;

c) la configuración de la Cuenta y la activación de funcionalidades realizadas por administradores autorizados;

d) las operaciones realizadas por los Usuarios Autorizados dentro de sus permisos;

e) las solicitudes remitidas desde el correo de contacto de la Cuenta o a través de los canales habilitados por MIND2; y

f) cualesquiera instrucciones adicionales aceptadas por escrito o por medios electrónicos.

MIND2 tratará los datos únicamente conforme a dichas instrucciones, incluidas las relativas a comunicaciones, transferencias internacionales, conservación, devolución y supresión.

MIND2 no podrá:

a) utilizar los datos para publicidad propia;

b) venderlos, alquilarlos o ponerlos a disposición de terceros para sus finalidades;

c) elaborar perfiles para fines propios;

d) entrenar modelos de inteligencia artificial o sistemas de aprendizaje automático con datos personales del Cliente; ni

e) combinar los datos con información de otros clientes para identificar, perfilar o adoptar decisiones sobre personas físicas.

El Cliente autoriza a MIND2 a realizar operaciones de agregación y anonimización irreversible con la finalidad exclusiva de medir, proteger y mejorar el Servicio, siempre que:

a) la anonimización sea efectiva;

b) no sea razonablemente posible identificar o reidentificar al Cliente ni a una persona física;

c) los resultados no se comuniquen de manera individualizada; y

d) MIND2 no conserve claves, correspondencias o elementos que permitan revertir la anonimización.

Si MIND2 considera que una instrucción infringe el RGPD, la LOPDgdd u otra norma de protección de datos, informará inmediatamente al Cliente y podrá suspender su ejecución hasta que este la confirme, modifique o retire. La suspensión se limitará al tratamiento afectado y no impedirá la adopción de medidas urgentes para proteger los datos.

Cuando MIND2 esté obligada a tratar o comunicar datos en virtud del Derecho de la Unión o de un Estado miembro, informará previamente al Cliente de dicha obligación, salvo que la norma aplicable lo prohíba por razones importantes de interés público.

5. Obligaciones del Cliente

Corresponde al Cliente:

a) determinar las finalidades y bases jurídicas de los tratamientos;

b) garantizar que la recogida, utilización y conservación de los datos sea lícita;

c) facilitar a las personas afectadas la información exigida por los artículos 13 y 14 RGPD;

d) atender las solicitudes de ejercicio de derechos;

e) aplicar los principios de licitud, lealtad, transparencia, limitación de la finalidad, minimización, exactitud y limitación del plazo de conservación;

f) establecer los plazos de conservación aplicables;

g) evaluar los riesgos del tratamiento y, cuando proceda, realizar una evaluación de impacto y una consulta previa;

h) cumplir las obligaciones laborales, de información y de participación de la representación de las personas trabajadoras;

i) verificar la necesidad, idoneidad y proporcionalidad de la geolocalización antes de activarla;

j) gestionar adecuadamente las altas, bajas, permisos y credenciales de sus Usuarios Autorizados;

k) mantener sus datos y configuraciones exactos y actualizados; y

l) comunicar a MIND2 las instrucciones necesarias para devolver, conservar, bloquear o suprimir los datos.

m) cuando utilice mecanismos SSO o integraciones con aplicaciones o sistemas propios o de terceros, garantizar la correcta gestión de las identidades, permisos y credenciales de sus Usuarios Autorizados, así como mantener actualizados y correctamente configurados los sistemas de autenticación bajo su control. El Cliente será responsable de determinar qué atributos o datos personales deben transmitirse a Fichajet mediante SSO y deberá limitar dicha transmisión a los datos adecuados, pertinentes y necesarios para la autenticación y prestación del Servicio.

El Cliente no cargará datos biométricos ni utilizará Fichajet para realizar identificación o autenticación biométrica mediante tratamiento de plantillas biométricas por parte de MIND2.

La eventual utilización de Face ID, huella u otra funcionalidad biométrica nativa del dispositivo solo podrá emplearse cuando la comprobación se realice localmente por el sistema operativo o proveedor del dispositivo y MIND2 no reciba, almacene ni pueda reconstruir la plantilla biométrica.

El Cliente limitará la incorporación de categorías especiales de datos a la información estrictamente necesaria y lícitamente tratada. En particular:

a) evitará cargar historias clínicas, diagnósticos, informes médicos completos o información sanitaria no necesaria;

b) revisará y, cuando proceda, ocultará o eliminará datos excesivos de los justificantes;

c) restringirá el acceso a dichos documentos a los Usuarios Autorizados que necesiten conocerlos; y

d) aplicará los plazos de conservación correspondientes.

Fichajet no está diseñado como repositorio de historias clínicas ni como sistema de seguimiento continuo de personas.

El Cliente responderá de la legalidad de las instrucciones, de los datos incorporados y del uso efectivo del Servicio, sin perjuicio de las obligaciones propias de MIND2 como encargado.

6. Obligaciones generales de MIND2

MIND2 se obliga a:

a) tratar los datos únicamente siguiendo instrucciones documentadas;

b) no comunicar los datos a terceros salvo instrucción del Cliente, autorización para subencargar o imposición legal;

c) limitar el acceso al personal cuya intervención sea necesaria;

d) garantizar que las personas autorizadas hayan asumido un compromiso de confidencialidad o estén sujetas a una obligación legal equivalente;

e) formar e instruir al personal autorizado en materia de protección de datos y seguridad;

f) implantar y mantener las medidas del Anexo II;

g) mantener un registro de las categorías de actividades de tratamiento realizadas por cuenta de sus clientes, cuando resulte exigible;

h) cooperar con la autoridad de control competente;

i) asistir al Cliente en el cumplimiento de sus obligaciones;

j) gestionar los subencargados conforme a la cláusula 12;

k) informar de las violaciones de seguridad conforme a la cláusula 9;

l) devolver o suprimir los datos al finalizar el Servicio; y

m) poner a disposición del Cliente la información necesaria para demostrar el cumplimiento de este Acuerdo.

7. Confidencialidad

MIND2 mantendrá el secreto y la confidencialidad sobre los datos personales tratados por cuenta del Cliente, incluso después de finalizar la relación contractual.

La obligación de confidencialidad comprenderá los datos, documentos, credenciales, configuraciones, registros, copias, extractos y cualquier información que permita inferir datos personales.

MIND2 mantendrá una relación actualizada de los perfiles o personas autorizadas para acceder a los datos y aplicará el principio de necesidad de conocer y mínimo privilegio.

El deber de confidencialidad no impedirá el acceso de auditores, asesores o proveedores debidamente autorizados y vinculados por obligaciones equivalentes, ni las comunicaciones exigidas por una norma o autoridad competente.

8. Seguridad del tratamiento

MIND2 aplicará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza,

alcance, contexto y fines del tratamiento y los riesgos para los derechos y libertades de las personas.

Las medidas inicialmente comprometidas se describen en el Anexo II e incluyen, al menos:

a) cifrado de las comunicaciones;

b) cifrado en reposo de los datos sensibles;

c) control de acceso basado en roles;

d) principio de mínimo privilegio;

e) autenticación reforzada para cuentas administrativas;

f) registro de accesos y modificaciones;

g) segregación lógica entre clientes;

h) copias de seguridad periódicas;

i) pruebas de restauración; y

j) procedimiento documentado de gestión de incidentes y violaciones de seguridad.

k) protección de los mecanismos de autenticación federada o SSO y de las interfaces de integración bajo el control de MIND2, incluyendo medidas destinadas a verificar la autenticidad e integridad de las comunicaciones y a prevenir accesos no autorizados.

MIND2 podrá modificar las medidas concretas para adaptarlas al estado de la técnica o a cambios de riesgo, siempre que la modificación no reduzca materialmente el nivel global de protección.

MIND2 verificará y evaluará periódicamente la eficacia de las medidas implantadas y corregirá, en un plazo razonable atendiendo a su gravedad, las deficiencias detectadas.

El Cliente reconoce que la seguridad del Servicio exige también medidas bajo su control, especialmente:

a) custodia de credenciales;

b) utilización de dispositivos y navegadores actualizados;

c) configuración adecuada de permisos;

d) revocación inmediata de accesos innecesarios;

e) prevención de cuentas administrativas compartidas; y

f) comunicación inmediata de pérdidas, accesos no autorizados o sospechas de compromiso.

g) configuración segura de sus proveedores de identidad y sistemas SSO;

h) gestión adecuada de altas, bajas, roles y permisos de los Usuarios Autorizados en dichos sistemas; y

i) revocación inmediata de accesos cuando una persona deje de estar autorizada para utilizar Fichajet.

9. Quiebras de la seguridad de los datos personales

MIND2 notificará al Cliente cualquier violación de la seguridad que afecte a datos tratados por su cuenta sin dilación indebida y, cuando sea posible, dentro de las setenta y dos horas siguientes a tener constancia de ella.

La comunicación inicial incluirá, en la medida en que la información esté disponible:

a) fecha y hora de detección y, si se conoce, de inicio y finalización;

b) descripción de la naturaleza del incidente;

c) sistemas, servicios o funcionalidades afectados;

d) categorías y número aproximado de interesados;

e) categorías y número aproximado de registros afectados;

f) posibles consecuencias;

g) medidas adoptadas o propuestas para contener, investigar y remediar el incidente;

h) medidas recomendadas al Cliente; e

i) identidad y datos de contacto del punto de contacto de MIND2.

Cuando no resulte posible facilitar toda la información simultáneamente, MIND2 la proporcionará de forma gradual sin dilación indebida.

MIND2:

a) adoptará medidas inmediatas de contención y mitigación;

b) preservará las evidencias pertinentes;

c) documentará los hechos, efectos y medidas correctivas;

d) colaborará con el Cliente en el análisis del riesgo;

e) facilitará la información razonablemente necesaria para las notificaciones de los artículos 33 y 34 RGPD; y

f) informará de la evolución y cierre del incidente.

Corresponde al Cliente decidir si debe notificarse la violación a una autoridad de control o comunicarse a las personas afectadas. MIND2 no realizará dichas comunicaciones por cuenta del Cliente salvo instrucción expresa o imposición legal.

La notificación de un incidente no supondrá por sí sola reconocimiento de responsabilidad por ninguna de las Partes.

10. Ejercicio de derechos

Cuando MIND2 reciba directamente una solicitud de acceso, rectificación, supresión, oposición, limitación, portabilidad o relativa a decisiones automatizadas que se refiera a tratamientos realizados por cuenta del Cliente:

a) no responderá sobre el fondo salvo instrucción expresa del Cliente;

b) remitirá la solicitud al Cliente sin dilación indebida y, como máximo, dentro de los dos días hábiles siguientes a su recepción; y

c) conservará evidencia de la remisión.

MIND2 asistirá al Cliente, teniendo en cuenta la naturaleza del tratamiento, mediante medidas técnicas y organizativas apropiadas, incluyendo, cuando sea posible:

a) búsqueda y localización de datos;

b) exportación en un formato estructurado;

c) rectificación o actualización;

d) limitación temporal de accesos o tratamientos;

e) supresión;

f) recuperación de registros de auditoría; y

g) información sobre destinatarios o subencargados.

El Cliente será responsable de verificar la identidad del solicitante, valorar la procedencia del derecho y emitir la respuesta dentro del plazo legal.

Cuando una solicitud requiera desarrollos específicos no incluidos en las funcionalidades ordinarias, las Partes acordarán previamente su alcance, plazo y, en su caso, costes, sin que ello permita a MIND2 dejar de prestar la asistencia legalmente exigible.

11. Asistencia en el cumplimiento normativo

MIND2 ayudará al Cliente a cumplir las obligaciones previstas en los artículos 32 a 36 RGPD, teniendo en cuenta la naturaleza del tratamiento y la información disponible.

En particular, facilitará información razonablemente necesaria sobre:

a) arquitectura y funcionamiento relevante del Servicio;

b) ubicación de los datos;

c) medidas de seguridad;

d) subencargados;

e) transferencias internacionales;

f) conservación y supresión;

g) incidentes y continuidad; y

h) riesgos conocidos asociados a las funcionalidades contratadas.

Cuando el Cliente deba realizar una evaluación de impacto, MIND2 proporcionará la información que obre en su poder sobre el tratamiento efectuado mediante Fichajet. La determinación de la necesidad de la evaluación, su elaboración y la decisión sobre la puesta en marcha del tratamiento corresponden al Cliente.

Cuando proceda una consulta previa ante la autoridad de control, MIND2 colaborará en el ámbito de sus funciones y facilitará la información técnica razonablemente solicitada.

MIND2 informará al Cliente, salvo prohibición legal, de cualquier requerimiento de una autoridad pública relacionado específicamente con los datos tratados por su cuenta.

12. Subencargados

El Cliente concede a MIND2 una autorización general y escrita para recurrir a los subencargados identificados en el Anexo III.

MIND2 informará al Cliente de cualquier incorporación o sustitución prevista con una antelación mínima de treinta días naturales. La comunicación identificará, al menos:

a) razón social;

b) servicio prestado;

c) categorías de datos o tratamientos afectados;

d) país o países desde los que se prestará el servicio;

e) ubicación prevista de los datos; y

f) mecanismo de transferencia internacional, cuando proceda.

El Cliente podrá oponerse dentro de los quince días naturales siguientes, siempre que invoque motivos razonables, concretos y documentados relacionados con la protección de datos.

Ante una oposición, las Partes intentarán adoptar una solución razonable, que podrá consistir en:

a) no utilizar al subencargado respecto del Cliente;

b) aplicar garantías adicionales;

c) ofrecer una alternativa técnicamente viable; o

d) cuando no exista alternativa razonable, resolver la parte afectada del Servicio.

Por razones urgentes de seguridad, continuidad o cumplimiento legal, MIND2 podrá sustituir provisionalmente un subencargado sin observar íntegramente el plazo de preaviso, informando al Cliente tan pronto como resulte posible y permitiendo posteriormente el ejercicio de oposición.

MIND2 formalizará con cada subencargado un contrato escrito que le imponga obligaciones de protección de datos sustancialmente equivalentes a las asumidas en este Acuerdo.

MIND2 seguirá siendo plenamente responsable frente al Cliente del cumplimiento de las obligaciones del subencargado en relación con el tratamiento encomendado.

Un proveedor que no tenga acceso real o potencial a datos personales del Cliente y que no realice operaciones de tratamiento por cuenta de este no tendrá la consideración de subencargado a estos efectos.

13. Ubicación y transferencias internacionales

La infraestructura principal de producción de Fichajet se alojará en España.

En la fecha de esta versión no se prevén transferencias internacionales de datos fuera del Espacio Económico Europeo.

MIND2 no transferirá datos ni permitirá su acceso desde un tercer país salvo que:

a) resulte necesario para prestar el Servicio;

b) informe previamente al Cliente;

c) cuente con una instrucción o autorización válida;

d) exista un instrumento conforme al capítulo V RGPD; y

e) se hayan evaluado y aplicado, cuando proceda, medidas complementarias.

La utilización de cláusulas contractuales tipo no eximirá a MIND2 de evaluar si la legislación y prácticas del país de destino pueden afectar a la eficacia de las garantías.

Ante una solicitud de acceso de una autoridad de un tercer país, MIND2, en la medida legalmente permitida:

a) informará al Cliente;

b) verificará la competencia y validez de la solicitud;

c) impugnará las solicitudes manifiestamente ilícitas o desproporcionadas;

d) limitará la comunicación a los datos estrictamente necesarios; y

e) documentará la actuación realizada.

14. Información, demostración del cumplimiento y auditorías

MIND2 pondrá a disposición del Cliente la información necesaria para demostrar el cumplimiento del artículo 28 RGPD y de este Acuerdo.

La acreditación podrá realizarse inicialmente mediante:

a) políticas y procedimientos;

b) cuestionarios de seguridad;

c) descripciones de medidas técnicas y organizativas;

d) informes de auditoría independientes;

e) certificados vigentes;

f) resultados resumidos de pruebas; y

g) documentación de subencargados y transferencias.

Cuando la documentación anterior no resulte suficiente, el Cliente podrá realizar una auditoría por sí mismo o mediante un auditor independiente sujeto a confidencialidad.

Salvo incidente grave, requerimiento de una autoridad o indicios razonables de incumplimiento:

a) la auditoría se realizará como máximo una vez al año;

b) se notificará con al menos treinta días naturales de antelación;

c) se efectuará durante horario laboral;

d) no interferirá de forma irrazonable en la prestación del Servicio; y

e) se limitará a sistemas, procesos y documentación relevantes para los datos del Cliente.

La auditoría no dará derecho a acceder a:

a) datos de otros clientes;

b) secretos empresariales no necesarios;

c) código fuente;

d) credenciales o claves criptográficas;

e) información cuya revelación genere un riesgo de seguridad; ni

f) documentación respecto de la cual MIND2 esté vinculada por una obligación de confidencialidad frente a terceros.

Los costes ordinarios de la auditoría serán asumidos por el Cliente. MIND2 asumirá los costes razonables directamente vinculados a la corrección cuando la auditoría revele un incumplimiento material imputable a MIND2.

MIND2 corregirá en un plazo razonable las deficiencias acreditadas, atendiendo a su gravedad, riesgo y complejidad técnica.

15. Devolución, recuperación, supresión y bloqueo

Durante la vigencia del Servicio, el Cliente podrá utilizar las funciones de exportación disponibles.

En los supuestos de cambio de proveedor, portabilidad o salida, resultará aplicable el procedimiento previsto en las Condiciones de Contratación.

Tras la finalización del periodo transitorio o, cuando no exista proceso de cambio, tras la terminación del Servicio, el Cliente dispondrá de un periodo mínimo de treinta días naturales para recuperar sus datos mediante acceso de solo lectura o un medio equivalente.

El Cliente comunicará a MIND2, antes de finalizar dicho periodo, si opta por:

a) la devolución de los datos;

b) su entrega a un nuevo proveedor técnicamente identificado; o

c) su supresión.

Cuando el Cliente no comunique una opción dentro del plazo, se entenderá que instruye la supresión, sin perjuicio de las obligaciones legales de conservación.

La devolución se efectuará, según la naturaleza de la información, mediante los formatos disponibles en el Servicio, incluyendo CSV o XLSX para datos estructurados, PDF para informes y formato original o ZIP para documentos cargados.

Completada la devolución o supresión, MIND2 eliminará las copias existentes en los sistemas de

producción, salvo que:

a) una norma exija su conservación; o

b) proceda el bloqueo para atender posibles responsabilidades.

Las copias de seguridad:

a) quedarán excluidas del uso ordinario;

b) permanecerán protegidas por las medidas de seguridad aplicables;

c) solo podrán restaurarse por razones de continuidad o seguridad;

d) volverán a quedar sujetas a la instrucción de supresión tras cualquier restauración; y

e) se sobrescribirán de forma segura dentro de su ciclo ordinario de rotación, cuyo plazo máximo será de treinta días naturales.

MIND2 podrá conservar debidamente bloqueados los datos estrictamente necesarios mientras puedan derivarse responsabilidades de la relación con el Cliente. Durante el bloqueo no podrán ser tratados para ninguna otra finalidad.

Cuando una norma obligue a conservar datos, MIND2 los devolverá al Cliente siempre que resulte técnicamente posible. Si debiera conservarlos directamente, los mantendrá bloqueados y limitará el acceso a las personas autorizadas para atender la obligación.

MIND2 emitirá, a solicitud del Cliente, confirmación de la supresión realizada, sin que sea necesario revelar información que comprometa la seguridad de sus sistemas.

El Cliente es responsable de garantizar la conservación de los registros de jornada durante el plazo legal aplicable, actualmente cuatro años, y de exportarlos antes de la supresión definitiva cuando sea necesario.

Los datos tratados por MIND2 como responsable independiente, tales como facturas, evidencias de contratación o comunicaciones contractuales, no se regirán por esta cláusula, sino por su propia base jurídica y plazo de conservación.

16. Comunicaciones y puntos de contacto

Las comunicaciones relativas a este Acuerdo se remitirán:

A MIND2: admin@mind2creations.com

Al Cliente: dirección electrónica asociada a la Cuenta o la identificada en la Confirmación de Contratación.

El Cliente mantendrá actualizado su correo de contacto y designará, cuando sea posible, una persona responsable de privacidad o seguridad.

Las comunicaciones sobre incidentes de seguridad se identificarán como urgentes y se remitirán al contacto designado por el Cliente.

Las Partes conservarán evidencias electrónicas de las instrucciones, comunicaciones, aceptaciones, cambios de versión y notificaciones relevantes.

17. Responsabilidad

Cada Parte responderá del cumplimiento de las obligaciones que le correspondan conforme al RGPD, la LOPDgdd, este Acuerdo y las instrucciones válidas.

MIND2 responderá de los daños causados por tratamientos en los que:

a) incumpla obligaciones dirigidas específicamente a los encargados;

b) actúe al margen o en contra de instrucciones lícitas; o

c) determine fines o medios esenciales propios.

El Cliente responderá de los daños derivados de:

a) instrucciones ilícitas;

b) ausencia de base jurídica;

c) falta de información a las personas afectadas;

d) configuración desproporcionada de funcionalidades;

e) incorporación de datos excesivos o innecesarios;

f) utilización indebida de geolocalización o categorías especiales; o

g) incumplimiento de sus obligaciones laborales y de conservación.

Cualquier limitación de responsabilidad prevista en las Condiciones de Contratación se aplicará únicamente en la medida permitida por la normativa y no limitará los derechos de las personas afectadas ni las potestades de las autoridades de control.

18. Modificaciones

MIND2 podrá actualizar este Acuerdo para adaptarlo a cambios normativos, resoluciones de autoridades, modificaciones técnicas o evolución del Servicio.

Las modificaciones no podrán reducir materialmente el nivel de protección ni alterar retroactivamente el tratamiento ya realizado.

Los cambios sustanciales se notificarán con al menos treinta días naturales de antelación. El Cliente podrá resolver la contratación antes de su entrada en vigor cuando el cambio perjudique materialmente sus derechos y no venga impuesto por una norma.

Las actualizaciones del Anexo III se regirán por el procedimiento específico de subencargados.

19. Vigencia y terminación

Este Acuerdo permanecerá vigente mientras MIND2 trate datos personales por cuenta del Cliente.

Las obligaciones de confidencialidad, devolución, supresión, bloqueo, auditoría y responsabilidad subsistirán después de la terminación en cuanto resulte necesario.

La terminación de las Condiciones de Contratación determinará la finalización del encargo, sin perjuicio de los periodos de transición, recuperación y rotación de copias de seguridad.

20. Legislación y jurisdicción

El Acuerdo se regirá por el RGPD, la LOPDGDD y la legislación española aplicable.

Las controversias se someterán a los juzgados y tribunales establecidos en las Condiciones de Contratación, sin perjuicio de las competencias de las autoridades de protección de datos y de cualquier fuero imperativo.

El Responsable del Tratamiento: [*]NIF:[*] Fdo.: [*]	**El Encargado del Tratamiento: MIND2 CREATIONS, S.L., NIF: B76114545 Fdo.: Gregorio Mayor Ibeas**

Anexo I.- Descripción del tratamiento

1. Servicio y objeto

Prestación de Fichajet como aplicación web SaaS para la gestión del registro de jornada y de las demás funcionalidades incluidas en el Plan contratado por el Cliente.

2. Finalidades

Gestión del registro horario; horarios y turnos; calendarios; libranzas, vacaciones, permisos y ausencias; Usuarios Autorizados; geolocalización puntual asociada al fichaje; documentos laborales incorporados por el Cliente; generación de informes y exportaciones; soporte, seguridad, copias de respaldo, continuidad y recuperación; autenticación y acceso mediante SSO e integración con aplicaciones o sistemas del Cliente, cuando dicha funcionalidad se encuentre habilitada.

3. Operaciones de tratamiento

Recogida, registro, estructuración, consulta, modificación, almacenamiento, conservación, recuperación, cotejo, generación de informes, exportación, puesta a disposición de Usuarios Autorizados, copia de seguridad, restauración, limitación, bloqueo, devolución y supresión.

4. Frecuencia

Tratamiento regular y continuado durante la vigencia del Servicio, con operaciones puntuales de soporte, exportación, recuperación o supresión.

5. Categorías de interesados

a) Personas trabajadoras actuales o anteriores del Cliente.

b) Profesionales, autónomos o colaboradores respecto de los cuales el Cliente gestione jornada, horarios o asistencia.

c) Administradores de Cuenta y Usuarios Autorizados.

d) Representantes o personal interno del Cliente cuyos datos formen parte de los contenidos gestionados por cuenta de este.

6. Categorías de datos personales

Datos identificativos: nombre, apellidos, identificador interno, número de empleado, DNI/NIE/NIF y otros datos equivalentes.

Datos de contacto: correo electrónico profesional, teléfono profesional y datos de contacto incorporados por el Cliente.

Datos profesionales y laborales: empresa, centro de trabajo, departamento, puesto, función, relación profesional, calendario, turno, horario, libranzas, vacaciones, permisos, ausencias e incidencias.

Registro de jornada: fecha y hora de entrada y salida, duración, pausas, rectificaciones, motivos de corrección, validaciones y trazabilidad asociada.

Geolocalización: coordenadas, ubicación o comprobación de localización obtenida puntualmente en el momento del fichaje cuando el Cliente habilite esta función. No comprende seguimiento continuo.

Datos técnicos: dirección IP, dispositivo, navegador, fecha y hora de acceso, registros de actividad, eventos de seguridad, incidencias técnicas y registros de auditoría.

Datos documentales: justificantes, nóminas y demás documentos cargados por el Cliente cuando su plan

incluya almacenamiento documental.

Datos económicos, laborales o de Seguridad Social: los que puedan aparecer en nóminas u otros documentos incorporados por el Cliente.

Datos de autenticación y acceso: nombre de usuario, identificadores internos o federados, identificador del proveedor de identidad, tokens de sesión o autenticación, perfil, rol, permisos, registros de autenticación y demás atributos estrictamente necesarios para gestionar el acceso mediante credenciales propias o mediante SSO. No se incluirán secretos, contraseñas o credenciales completas en las exportaciones.

7. Categorías especiales

Podrán tratarse incidentalmente datos de salud u otras categorías especiales contenidos en justificantes o documentos laborales únicamente cuando:

a) el Cliente disponga de una excepción válida del artículo 9.2 RGPD;

b) sean estrictamente necesarios;

c) la funcionalidad correspondiente esté habilitada; y

d) se apliquen medidas de acceso y conservación reforzadas.

El Servicio no deberá utilizarse para almacenar historias clínicas, información diagnóstica extensa ni documentos sanitarios innecesarios.

8. Exclusión de datos biométricos

MIND2 no tratará plantillas faciales, dactilares ni otros datos biométricos dirigidos a identificar de manera unívoca a una persona.

La eventual autenticación mediante Face ID o huella del dispositivo deberá producirse localmente, sin transmisión a MIND2 de la plantilla biométrica.

9. Decisiones automatizadas

MIND2 no adoptará por cuenta propia decisiones basadas únicamente en tratamientos automatizados que produzcan efectos jurídicos o afecten significativamente de manera similar a los interesados.

10. Volumen aproximado

El volumen dependerá del plan contratado, del número de personas trabajadoras, de los centros de trabajo y de la capacidad documental habilitada.

11. Duración y conservación

Los plazos aplicables a cada categoría serán determinados por el Cliente de conformidad con la normativa aplicable. Durante la vigencia de la suscripción, los registros de jornada generados mediante Fichajet se mantendrán accesibles a través del Servicio durante el plazo previsto en las Condiciones de Contratación, sin perjuicio de que la obligación legal de garantizar su conservación durante cuatro años corresponda al Cliente en su condición de empleador.

12. Ubicación

Infraestructura principal de producción en España. Los servicios auxiliares y ubicaciones adicionales serán los indicados en el Anexo III.

13. Transferencias internacionales

No previstas fuera del Espacio Económico Europeo en la fecha de esta versión.

Anexo II.- Medidas técnicas y organizativas

1. Organización, políticas y personal

1.1. Existencia de políticas internas de seguridad y protección de datos proporcionales al riesgo.

1.2. Acceso limitado a personal autorizado que necesite tratar los datos para sus funciones.

1.3. Compromisos de confidencialidad y formación periódica.

1.4. Procedimientos de alta, modificación y revocación de permisos.

1.5. Registro y revisión de perfiles privilegiados.

1.6. Gestión documentada de incidentes y violaciones de seguridad.

2. Control de acceso

2.1. Control de acceso basado en roles.

2.2. Aplicación del principio de mínimo privilegio.

2.3. Cuentas nominales para el personal autorizado.

2.4. Autenticación reforzada para cuentas administrativas.

2.5. Revocación de accesos cuando dejen de ser necesarios.

2.6. Medidas para impedir accesos entre entornos de clientes distintos.

2.7. Cuando se utilicen mecanismos SSO, validación segura de las solicitudes o respuestas de autenticación recibidas de proveedores de identidad autorizados.

2.8. Aplicación de controles destinados a evitar la reutilización indebida, alteración o suplantación de tokens o mecanismos equivalentes de autenticación, de acuerdo con la arquitectura técnicamente utilizada.

2.9. Limitación de los atributos recibidos mediante SSO a aquellos necesarios para la autenticación, autorización y prestación de las funcionalidades contratadas.

3. Protección criptográfica

3.1. Cifrado de las comunicaciones mediante TLS o protocolo equivalente actualizado.

3.2. Cifrado en reposo de los datos considerados sensibles.

3.3. Gestión restringida de claves y secretos técnicos.

3.4. No almacenamiento de contraseñas o PIN en texto claro, cuando técnicamente resulten aplicables mecanismos de derivación o hash seguro.

3.5. Protección mediante cifrado de las comunicaciones utilizadas en los procesos de autenticación SSO y en las interfaces de integración con aplicaciones o sistemas externos.

4. Segregación y arquitectura

4.1. Segregación lógica de los datos de cada cliente en la arquitectura multiempresa.

4.2. Controles destinados a impedir consultas, exportaciones o modificaciones cruzadas.

5. Registro y monitorización

5.1. Registro de accesos y modificaciones relevantes.

5.2. Registro de operaciones administrativas y eventos de seguridad.

5.3. Protección de los registros frente a alteración o acceso no autorizado.

5.4. Revisión de eventos anómalos.

6. Copias de seguridad y continuidad

6.1. Copias de seguridad periódicas.

6.2. Protección de las copias mediante controles de acceso y, cuando proceda, cifrado.

6.3. Pruebas periódicas de restauración.

6.4. Procedimientos para recuperar la disponibilidad y acceso a los datos tras un incidente.

6.5. Separación lógica o física suficiente entre producción y copias.

6.6. Ciclo máximo de rotación y sobreescritura segura de 30 días.

6.7. Objetivos internos de recuperación y pérdida máxima admisible de datos: RTO 24 horas / RPO 24 horas.

7. Gestión de vulnerabilidades y cambios

7.1. Aplicación de actualizaciones de seguridad en función de la criticidad y riesgo.

7.2. Gestión de dependencias y componentes de terceros.

7.3. Corrección priorizada de vulnerabilidades críticas.

7.4. Revisión de seguridad antes de cambios materiales de arquitectura.

7.5. Revisión de seguridad de las integraciones SSO y de los cambios materiales que afecten a los mecanismos de autenticación o autorización.

8. Gestión de incidentes

8.1. Canales internos de detección y escalado.

8.2. Procedimientos de contención, análisis, remediación y recuperación.

8.3. Preservación de evidencias.

8.4. Comunicación al Cliente conforme a la cláusula 9.

8.5. Revisión posterior y adopción de medidas preventivas.

9. Disponibilidad y resiliencia

9.1. Monitorización razonable de la disponibilidad del Servicio.

9.2. Mecanismos de restauración ante fallos físicos o técnicos.

9.3. Procedimientos de continuidad proporcionados a la criticidad.

9.4. Comunicación de indisponibilidades relevantes conforme a las Condiciones de Contratación.

10. Supresión y eliminación

10.1. Supresión lógica de datos en producción tras finalizar el periodo de recuperación.

10.2. Sobrescritura segura de copias dentro del ciclo de rotación.

10.3. Destrucción o borrado seguro de soportes cuando sean retirados.

10.4. Bloqueo de datos conservados para atender responsabilidades.

11. Seguridad física y alojamiento

11.1. Alojamiento de la infraestructura principal de producción en España.

11.2. Controles físicos de acceso, suministro eléctrico, climatización, detección de incendios y continuidad aplicables en el centro de datos.

12. Revisión

12.1. Revisión periódica de la eficacia de las medidas.

12.2. Adaptación cuando cambien el riesgo, la tecnología, las funcionalidades o las categorías de datos.

12.3. Documentación de cambios materiales y, cuando proceda, comunicación al Cliente.

Anexo III.- Subencargados autorizados

Subencargado	Servicio	Tratamientos	Ubicación	Garantías TID
Raiola Networks, S.L.	Alojamiento e infraestructura Copias de seguridad o continuidad	Todos los del Anexo I	España	N/A

Firmas

En prueba de conformidad, MIND2 CREATIONS, S.L. suscribe el presente Acuerdo de Tratamiento de Datos Personales. El Cliente lo acepta mediante la aceptación electrónica de las Condiciones de contratación acreditada en su Confirmación de Contratación; este ejemplar se facilita para que pueda completar sus datos, firmarlo y conservarlo como constancia escrita del encargo (artículo 28.3 del RGPD).

Por el Encargado del Tratamiento

_____

Gregorio Mayor Ibeas
Representante legal de MIND2 CREATIONS, S.L. · NIF B76114545
Arrecife de Lanzarote, 3 de septiembre de 2026

Por el Cliente (Responsable del Tratamiento)

A completar y firmar por el Cliente.

Razón social o nombre y apellidos

NIF / NIE / CIF

Domicilio

Nombre y apellidos de quien firma, y cargo

Correo electrónico de contacto en materia de protección de datos

Lugar y fecha

Firma y, en su caso, sello