Acuerdo de encargo de tratamiento de datos personales

Versión: dpa-2026-07-20-v1 **Vigente desde:** 20 de julio de 2026 **Aplicación:** este acuerdo se aplica a los clientes profesionales y únicamente a los tratamientos en los que MicroSmart trate datos personales por cuenta del cliente.

1. Partes, roles y prevalencia

El **Responsable** es la empresa o profesional identificado en la contratación que utiliza MicroSmart para tratar datos de sus contactos, personal o clientes finales. El **Encargado** es MICROSMART, S.L., NIF B93791218, con domicilio en C/ José María Gómez Jane 2, Esc. 1, 1.º, Pta. 12, 45211 Recas (Toledo), España.

Este acuerdo desarrolla el artículo 28 del RGPD y prevalece sobre las condiciones generales respecto de los tratamientos por cuenta del Responsable. No convierte en encargo los tratamientos propios de MicroSmart -cuenta, facturación, seguridad, defensa jurídica y comunicaciones propias-, que se rigen por la Política de privacidad.

2. Objeto, duración y naturaleza

El Encargado tratará los datos necesarios para prestar las capacidades contratadas y activadas durante la vigencia del servicio y los periodos limitados de devolución, supresión y conservación de copias técnicas. La naturaleza puede incluir recogida, registro, organización, consulta, transmisión por los canales configurados, generación asistida por IA, almacenamiento, recuperación, bloqueo, exportación y supresión.

El Encargado no venderá los datos ni los tratará para fines propios incompatibles. Las instrucciones documentadas comprenden el contrato, las configuraciones válidas, las acciones de usuarios autorizados y las solicitudes posteriores legalmente admisibles.

3. Instrucciones y legalidad

El Encargado tratará los datos únicamente conforme a instrucciones documentadas, salvo obligación del Derecho de la Unión o de los Estados miembros; limitará el acceso a personas autorizadas sujetas a confidencialidad; mantendrá el registro de categorías de actividades exigible; y pondrá a disposición del Responsable la información razonablemente necesaria para demostrar cumplimiento y permitir auditorías proporcionadas. Si considera que una instrucción infringe la normativa, lo comunicará sin demora.

El Responsable garantiza que dispone de base jurídica, informa a las personas interesadas, configura plazos y canales, atiende derechos y no imparte instrucciones ilícitas. En campañas, llamadas, WhatsApp y redes, el Responsable conserva la responsabilidad sobre destinatarios, listas, identificación y oposiciones.

4. Seguridad

El Encargado aplica las medidas técnicas y organizativas del Anexo III, adecuadas al riesgo conforme al artículo 32 del RGPD. El Responsable aplicará medidas apropiadas en sus dispositivos, integraciones, credenciales, personal y exportaciones.

5. Violaciones de seguridad

El Encargado notificará al Responsable sin dilación indebida tras conocer una violación que afecte a datos tratados por su cuenta y aportará la información disponible sobre su naturaleza, categorías, volumen aproximado, consecuencias y medidas adoptadas o previstas. La información se actualizará de forma progresiva. El Responsable decide las notificaciones a autoridad e interesados, salvo obligación directa del Encargado.

6. Derechos y cooperación

Cuando reciba una solicitud vinculada a datos del Responsable, el Encargado la remitirá o ayudará a atenderla mediante las capacidades disponibles, considerando la naturaleza del tratamiento y la información disponible. También asistirá razonablemente en evaluaciones de impacto, consultas previas, seguridad y cumplimiento. La asistencia extraordinaria podrá presupuestarse si no deriva de un incumplimiento del Encargado y se informa antes.

7. Subencargados

El Responsable concede autorización general para usar subencargados dentro de las categorías vigentes descritas en el documento de categorías de subencargados y servicios conectados. El Encargado impondrá las obligaciones exigidas por el artículo 28 del RGPD y seguirá respondiendo frente al Responsable en los términos legales.

Los cambios materiales se comunicarán con antelación razonable. El Responsable podrá oponerse por motivos documentados de protección de datos. Las partes buscarán una alternativa razonable; si no existe, podrá desactivarse o terminarse la capacidad afectada sin penalización desproporcionada.

8. Transferencias internacionales

Antes de incorporar un proveedor con transferencia o acceso internacional, el Encargado identificará y documentará el mecanismo aplicable -decisión de adecuación, cláusulas contractuales tipo, normas corporativas vinculantes u otro permitido- y, cuando corresponda, su evaluación y medidas complementarias. La relación pública identifica categorías y módulos; los datos nominales y la arquitectura se mantienen en el registro contractual protegido de MicroSmart.

9. Devolución, portabilidad y supresión

Al terminar el servicio, y a elección documentada del Responsable, el Encargado devolverá los datos personales disponibles y suprimirá las copias existentes, salvo conservación exigida por el Derecho aplicable. La devolución se realizará por el medio documentado para los datos disponibles en MicroSmart.

Las copias técnicas se mantendrán bloqueadas, protegidas y fuera del uso ordinario hasta su eliminación conforme al ciclo de conservación indicado en el Anexo III. La devolución no comprende datos controlados directamente por el Responsable ni permite garantizar supresión inmediata en sistemas de terceros; se respetarán sus contratos y mecanismos técnicos aplicables.

10. Auditoría

El Responsable podrá solicitar evidencias y, si son insuficientes, una auditoría razonable con preaviso, alcance acordado, confidencialidad y sin comprometer a otros clientes. Se priorizarán certificaciones, informes y auditorías remotas. El Responsable asumirá costes extraordinarios salvo incumplimiento material acreditado.

11. Responsabilidad y terminación

La responsabilidad se distribuye conforme al RGPD y al contrato principal, sin limitar los derechos de las personas. Un incumplimiento esencial no subsanado permite terminar la parte afectada. Las obligaciones de confidencialidad, devolución y responsabilidad sobreviven cuando corresponda.

Anexo I - Detalles del tratamiento

Finalidad

Prestar al Responsable una plataforma de gestión y automatización empresarial asistida por IA mediante las capacidades que active.

Personas interesadas

Contactos, clientes y potenciales clientes; proveedores; empleados y colaboradores del Responsable; usuarios autorizados; y personas que llaman, escriben, reservan, compran, comentan o interactúan con sus canales.

Categorías de datos

Identificación y contacto; datos de relación comercial; mensajes y contenido; voz, grabaciones y transcripciones si se activan; solicitudes, citas, reservas y pedidos; productos o servicios consultados; perfiles CRM y seguimientos; contenidos de redes; y datos de uso, dispositivo y seguridad.

No se prevé tratar de forma sistemática categorías especiales de datos ni datos penales. Su uso exige instrucción, base y garantías específicas antes de introducirlos.

Operaciones y módulos

- WhatsApp, panel y voz: recibir, conservar, analizar, responder y ejecutar acciones autorizadas.
- CRM: registrar y consultar contactos, contexto y seguimientos.
- Inventario, servicios, materiales y web: buscar y transmitir información autorizada.
- Agenda, citas, reservas y pedidos: consultar disponibilidad, crear, modificar o cancelar según permisos y confirmaciones.
- Campañas y redes: preparar, publicar y atender comunicaciones bajo responsabilidad del Responsable.
- Informes, saldo y recargas: medir actividad y generar registros operativos y económicos.

Anexo II - Instrucciones especiales

- Solo se habilitan las herramientas activadas para la empresa.
- Las operaciones que modifican datos se ejecutan mediante los flujos autorizados de la plataforma y conservan trazabilidad.
- El Responsable configura los canales, redes, grupos, números autorizados y números de guardia que pueden actuar o recibir eventos.
- Las acciones de riesgo requieren las confirmaciones que establezca el producto.
- La IA no debe comunicar que una acción se ha realizado sin el resultado real de la herramienta.

Anexo III - Medidas técnicas y organizativas

Las medidas de este anexo se aplican dentro del alcance de los módulos activos y se revisan conforme al riesgo del servicio.

Área	Medidas aplicadas
Aislamiento y control de acceso	Separación lógica de los datos de cada cuenta y controles de acceso según las funciones autorizadas. Cada usuario solo accede a las funciones y datos que le corresponden.

Área	Medidas aplicadas
Comunicaciones y secretos	Medidas técnicas de protección de las comunicaciones acordes con el riesgo. Los secretos y credenciales de integración se gestionan como información confidencial y no se exponen en las respuestas de la plataforma.
Registro y trazabilidad	Registros de seguridad, auditoría y operación para investigar incidencias y comprobar acciones relevantes. Se conservan como máximo 12 meses, salvo incidente, obligación legal o retención ligada a un procedimiento.
Copias de seguridad	Cuando están habilitadas, existen copias rotativas de 48 horas, 14 días y 8 semanas. Las copias se mantienen protegidas y fuera del uso ordinario hasta su sobrescritura o eliminación.
Respuesta ante incidentes	Procedimientos de detección, análisis, contención y comunicación de incidentes. Las violaciones que afecten a datos del Responsable se comunican conforme a la cláusula 5.
Ejecución de acciones	Las operaciones que modifican datos se realizan mediante flujos autorizados que preservan el alcance de cada cuenta, las confirmaciones exigibles y la trazabilidad.
Acceso del proveedor	El acceso de MicroSmart se limita a personal autorizado que lo necesita para operar, soportar o asegurar el servicio y está sujeto a confidencialidad.
Conservación y salida	Datos de cuenta durante la relación y la prescripción aplicable; contenidos y conversaciones mientras la cuenta siga activa y el Responsable no los elimine y, tras terminar, hasta 30 días para exportación o devolución; grabaciones según la configuración y el proveedor aplicable. La supresión no se presenta como inmediata en copias técnicas o sistemas de terceros.

Anexo IV - Contactos

Las comunicaciones jurídicas y de privacidad al Encargado se dirigen a info@microsmart.es. El Responsable mantendrá actualizado su contacto contractual en la plataforma.

Fuentes oficiales

- RGPD, especialmente artículos 28 y 32 a 36 (https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa)
- AEPD: directrices para contratos entre responsables y encargados (https://www.aepd.es/documento/guia-directrices-contratos.pdf)
- Decisión 2021/915, cláusulas contractuales tipo entre responsables y encargados (https://eur-lex.europa.eu/eli/dec_impl/2021/915/oj/spa)
- Decisión 2021/914, cláusulas contractuales tipo (https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj/spa)