Contrato de encargo del tratamiento (art. 28 del RGPD)

Borrador preparado por el equipo técnico. Antes de firmarlo debe revisarlo la asesoría jurídica de Black Wings S.L. y la persona delegada de protección de datos del cliente.

1. Partes

- **Responsable del tratamiento:** el cliente (ayuntamiento, administración o empresa) que contrata Kalmee.
- **Encargado del tratamiento: BLACK WINGS, S.L.**, NIF B10991172, con domicilio en C/ Mirasol, 8, bajo, 46015 Valencia, inscrita en el Registro Mercantil de Valencia, hoja V-206055. Contacto: soporte@kalmee.com · +34 622 116 868. Marca comercial: Kalmee (kalmee.com).

2. Objeto, duración, naturaleza y finalidad

Concepto	Contenido
Objeto	Prestar el servicio Kalmee de gestión de colas y cita previa
Duración	La del contrato principal
Naturaleza	Alojamiento, registro, consulta, conservación, anonimización y supresión
Finalidad	Gestionar los turnos y las citas de atención al público del responsable

3. Datos y personas afectadas

Tratamiento	Personas afectadas	Datos
Cita previa	Ciudadanos o clientes que piden cita	Nombre y apellidos, correo electrónico, teléfono (opcional), DNI o NIE solo en los trámites que lo exigen, trámite, oficina y hora
Turnos sin cita	Personas que sacan turno en el kiosco	Ninguno: solo el número de turno y su trazabilidad (horas, mesa y servicio)
Derivaciones	Personas atendidas	Nota libre opcional del personal. No debe contener datos personales y se elimina al vencer el plazo de conservación
Usuarios del backoffice	Personal del responsable	Correo electrónico, nombre visible, rol y actividad de atención
Avisos de soporte	Personal del responsable	Correo electrónico y teléfono de contacto opcional

No se tratan categorías especiales de datos.

4. Obligaciones del encargado

1. Tratar los datos solo siguiendo las instrucciones documentadas del responsable, que son este contrato y la configuración que el responsable hace en la aplicación.
2. Exigir confidencialidad a todas las personas autorizadas a tratar los datos.
3. Aplicar las medidas de seguridad del apartado 6.
4. No recurrir a otro encargado sin autorización. Los subencargados autorizados son los del apartado 5, y cualquier cambio se avisa con 30 días para que el responsable pueda oponerse.
5. Ayudar al responsable a atender los derechos de las personas: acceso, rectificación, supresión, limitación, portabilidad y oposición.
6. Ayudar al responsable en las evaluaciones de impacto y en las consultas a la autoridad de control.
7. Notificar al responsable cualquier violación de seguridad sin dilación indebida, y en todo caso en un plazo de 24 horas desde que se conozca, con la información disponible.
8. Al terminar el servicio, devolver los datos o suprimirlos, a elección del responsable, en un plazo de 30 días, salvo obligación legal de conservarlos.
9. Poner a disposición del responsable la información necesaria para demostrar el cumplimiento y permitir auditorías razonables.

5. Subencargados

Todos tratan los datos en la Unión Europea o con garantías adecuadas: cláusulas contractuales tipo o el Marco de Privacidad de Datos UE-EE. UU.

Subencargado	Servicio	Ubicación de los datos
Supabase Inc.	Base de datos, autenticación y tiempo real	UE (París, eu-west-3)
Vercel Inc.	Alojamiento de la aplicación	Funciones en la UE (París, cdg1). Red de distribución global, sin almacenar datos personales
Resend Inc.	Envío de correos transaccionales: confirmación de cita y avisos	UE (Irlanda, eu-west-1)
Google LLC (Cloud Text-to-Speech)	Locuciones de la pantalla generadas una sola vez con textos genéricos (turno, letras y números)	No recibe datos personales

6. Medidas de seguridad

- **Aislamiento entre organizaciones.** Seguridad a nivel de fila en todas las tablas, con tests automáticos.
- **Superficies públicas.** Funcionan con enlaces secretos de 256 bits, revocables y con límite de peticiones. Nunca se abre el acceso anónimo a la base de datos.
- **Cifrado.** Tráfico cifrado (HTTPS con HSTS) y datos cifrados en reposo por el proveedor de base de datos.
- **Cabeceras de seguridad.** CSP, X-Frame-Options, Referrer-Policy y Permissions-Policy.
- **Minimización.** Las pantallas y el seguimiento no muestran datos personales. La cita pide solo lo necesario, y el DNI solo si el trámite lo exige.
- **Conservación.** Plazos configurables, con anonimización automática de las citas y supresión de las notas de derivación.
- **Copias de seguridad** diarias.
- **Gestión de accesos por roles.** La verificación en dos pasos para administradores está en desarrollo.

7. Plazos de conservación por defecto

Dato	Plazo	Cómo se aplica
Datos personales de la cita	365 días desde la cita (configurable de 30 a 3.650 días)	Anonimización automática con `purge_expired_personal_data()`
Notas de derivación	Según el plazo de la organización	Se suprimen
Turnos sin cita	Sin datos personales	Se conservan con fines estadísticos