# TRATAMIENTO DE DATOS PERSONALES DEL SERVICIO HORUS

(ALERTAS PERSONALES DE EMERGENCIA)

Anexo a la Política de Privacidad de SAFETROOP TECHNOLOGIES, S.L.

El presente Anexo forma parte integrante de la Política de Privacidad general de SAFETROOP TECHNOLOGIES, S.L. y regula de manera específica el tratamiento de datos personales realizado a través del servicio HORUS, dada la naturaleza especialmente sensible de los datos tratados y las finalidades de emergencia asociadas a dicho servicio.

# 1. DESCRIPCIÓN DEL SERVICIO HORUS

HORUS es un servicio de alerta personal diseñado para su utilización en situaciones de emergencia, riesgo o peligro para la integridad física del usuario. El servicio permite, mediante una activación voluntaria, expresa y consciente, el envío de una señal de auxilio que habilita determinadas funcionalidades avanzadas del dispositivo móvil del usuario con la finalidad exclusiva de gestionar la situación de emergencia.

El servicio HORUS no realiza ningún tratamiento de datos de forma continua, automática ni pasiva, quedando todas sus funcionalidades avanzadas desactivadas por defecto hasta la activación expresa por parte del usuario.

# 2. RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento de los datos personales tratados a través del servicio HORUS es:

**SAFETROOP TECHNOLOGIES, S.L.**
CIF: B44925204
Domicilio social: Carrer de L'Escorial 115, planta 5, puerta A, CP 08024, Barcelona (España)
Correo electrónico de contacto: info@safetroop.com

# 3. CATEGORÍAS DE DATOS PERSONALES TRATADOS

Exclusivamente en el momento en que el usuario activa manualmente una alerta HORUS, podrán tratarse las siguientes categorías de datos personales:

## a) Datos identificativos

- Nombre y apellidos
- Dirección postal
- Número de teléfono
- Dirección de correo electrónico

### b) Datos de localización

- Datos de geolocalización en tiempo real del dispositivo del usuario durante la activación de la alerta.

### c) Datos de audio y vídeo

- Imágenes y sonido captados por la cámara y el micrófono del dispositivo del usuario durante la gestión de la emergencia.

### d) Datos técnicos

- Dirección IP
- Identificadores del dispositivo
- Información técnica necesaria para la transmisión de la alerta y la comunicación con los servicios de emergencia.

## 4. FINALIDAD ESPECÍFICA DEL TRATAMIENTO

Los datos personales tratados a través del servicio HORUS se utilizarán exclusivamente para las siguientes finalidades:

- Gestionar y atender situaciones de emergencia comunicadas por el usuario.
- Permitir la localización inmediata del usuario durante una situación de riesgo.
- Facilitar la intervención de Fuerzas y Cuerpos de Seguridad, servicios de emergencia, protección civil u otras autoridades competentes.
- Proteger la vida, integridad física y seguridad del usuario.

Los datos no serán utilizados para finalidades comerciales, publicitarias ni analíticas.

## 5. BASE JURÍDICA DEL TRATAMIENTO

El tratamiento de datos personales en el servicio HORUS se legitima conforme a lo dispuesto en el artículo 6 del RGPD, en base a:

- El consentimiento explícito del usuario (art. 6.1.a RGPD), manifestado mediante la activación consciente del sistema de alerta.
- La protección de intereses vitales del interesado o de otras personas físicas (art. 6.1.d RGPD).

- Cuando resulte aplicable, el cumplimiento de una misión realizada en interés público por parte de las autoridades intervinientes (art. 6.1.e RGPD).

# 6. ACTIVACIÓN DEL SERVICIO Y CONTROL DEL USUARIO

La activación del tratamiento de datos en HORUS:

- Se produce únicamente mediante una acción voluntaria del usuario.
- No se activa por el mero uso o instalación de la aplicación.
- Puede ser finalizada por el usuario en cualquier momento, sin perjuicio de las obligaciones legales de conservación que puedan resultar aplicables.

# 7. TRATAMIENTO INCIDENTAL DE DATOS DE TERCEROS

Durante la activación de una alerta HORUS, pueden captarse de forma incidental imágenes o sonidos de terceras personas que se encuentren en el entorno del usuario. Dicho tratamiento:

- Se considera estrictamente accesorio y necesario para la gestión de la emergencia.
- Se limita a la finalidad de protección de intereses vitales.
- No será objeto de usos adicionales ni independientes.

# 8. DESTINATARIOS DE LOS DATOS

Los datos personales tratados a través de HORUS podrán ser comunicados, cuando resulte estrictamente necesario, a:

- Fuerzas y Cuerpos de Seguridad del Estado.
- Servicios de emergencia y protección civil.
- Autoridades judiciales o administrativas competentes.

Asimismo, determinados proveedores tecnológicos podrán acceder a los datos en calidad de Encargados del Tratamiento, conforme a contratos suscritos de acuerdo con el artículo 28 del RGPD.

# 9. VIDEOCOMUNICACIONES Y USO DE PLATAFORMAS DE TERCEROS

Las comunicaciones de audio y vídeo del servicio HORUS se realizan mediante plataformas tecnológicas de terceros, tales como Zoom Video Communications, Inc., que actúan como Encargados del Tratamiento, de conformidad con sus respectivos acuerdos de tratamiento de datos (DPA) y con las garantías exigidas por el RGPD.

SafeTroop mantiene en todo caso la condición de Responsable del Tratamiento.

# 10. PLAZO DE CONSERVACIÓN DE LOS DATOS

Los datos personales generados durante una alerta HORUS se conservarán:

- Durante el tiempo estrictamente necesario para la gestión de la emergencia.
- Posteriormente, durante los plazos legales de prescripción aplicables para la atención de posibles responsabilidades legales.
- Transcurridos dichos plazos, los datos serán bloqueados o suprimidos conforme a la normativa vigente.

# 11. MEDIDAS DE SEGURIDAD Y PRIVACIDAD DESDE EL DISEÑO

Dada la naturaleza especialmente sensible del tratamiento asociado a HORUS, que puede incluir datos identificativos, datos de localización en tiempo real, audio, vídeo, información sobre situaciones de emergencia y datos vinculados a colectivos vulnerables, SafeTroop ha implementado medidas técnicas y organizativas orientadas a garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y minimización del tratamiento.

En particular, se aplican las siguientes medidas:

## 1. Alojamiento de la información en entorno europeo

La plataforma se encuentra desplegada sobre Google Cloud Platform en la región europe-west1, Bélgica, manteniendo los principales servicios de tratamiento dentro del Espacio Económico Europeo. Los buckets de almacenamiento se encuentran igualmente configurados en entorno EU, reduciendo el riesgo de

transferencias internacionales no controladas.

## 2. Arquitectura segregada y reducción de superficie de exposición

La solución se organiza en componentes diferenciados para backend, paneles de administración y aplicaciones móviles. El backend expone distintos esquemas GraphQL separados para Connectpol, Proximity y Proximity/HORUS, cada uno con su propia clave de API.

Los servicios Cloud Run se encuentran configurados con acceso internal-and-cloud-load-balancing, evitando su exposición directa a Internet y canalizando el acceso a través del balanceador seguro.

## 3. Protección perimetral y control del tráfico

El acceso público se realiza mediante un Google Cloud Load Balancer con certificados SSL gestionados y política de seguridad Cloud Armor, incluyendo limitación de tráfico por IP y bloqueo automático cuando se superan los umbrales definidos. Esta medida contribuye a mitigar abusos, automatismos, ataques de fuerza bruta y tráfico anómalo.

## 4. Cifrado de las comunicaciones

Las comunicaciones externas se realizan mediante HTTPS con TLS 1.2 o superior. La política SSL aplicada deshabilita suites criptográficas débiles o basadas en intercambio RSA estático, priorizando suites ECDHE con forward secrecy.

Las comunicaciones internas entre Cloud Run, Cloud SQL, Cloud Storage, Secret Manager, Datastream y BigQuery se realizan mediante canales cifrados gestionados por Google Cloud.

## 5. Seguridad de la base de datos y almacenamiento

El acceso del backend a Cloud SQL se realiza mediante Cloud SQL Auth Proxy, ejecutado como sidecar dentro del mismo entorno Cloud Run. La aplicación se conecta al proxy por socket Unix local, evitando exposición directa de la base de datos a la red.

El acceso externo a Cloud SQL queda restringido a redes autorizadas y a las IPs estáticas de salida definidas para Cloud Run y el pipeline CI.

Los datos en reposo se encuentran cifrados mediante cifrado gestionado por Google. Además, Cloud SQL dispone de copias de seguridad diarias y binary log activado.

## 6. Separación entre información privada y pública

El sistema diferencia entre buckets de almacenamiento privados y públicos. El bucket privado se utiliza para ficheros internos, informes y adjuntos, mientras que el bucket público queda limitado a imágenes y activos públicos. Esta separación reduce el riesgo de exposición accidental de documentación sensible.

## 7. Gestión segura de secretos y credenciales

Las claves sensibles, incluyendo la clave privada RSA utilizada para la firma de JWT, se custodian en Google Secret Manager.

El acceso programático se realiza mediante cuentas de servicio específicas y restringidas, utilizadas desde Cloud Run y desde el pipeline de despliegue correspondiente. Las credenciales de acceso quedan limitadas a usuarios autorizados y al proceso de integración continua.

## 8. Autenticación reforzada y control de sesiones

El acceso a la plataforma se realiza mediante flujos de autenticación basados en códigos OTP enviados por SMS o email, con códigos de 6 dígitos, caducidad limitada a 3 minutos y número máximo de intentos.

Una vez validado el acceso, el sistema emite tokens JWT firmados con RS256 y expiración corta, junto con refresh tokens de alta entropía. Esta configuración limita el impacto de una eventual exposición de credenciales o tokens.

## 9. Control de autorización por roles y claves API

Toda petición GraphQL requiere una clave X-Api-Key específica del esquema correspondiente y, salvo los endpoints de autenticación, un token Bearer JWT válido.

El sistema aplica autorización mediante roles diferenciados, incluyendo perfiles como ADMIN, MANAGER, USER, PROXIMITY_MANAGER y GUEST. Las directivas de autorización validan tanto la autenticación como los permisos necesarios para cada operación.

## 10. Principio de minimización y privacidad por defecto

El sistema limita el acceso a la información a usuarios autenticados y autorizados según su rol, evitando accesos generalizados o innecesarios a datos personales o información sensible.

En el caso del panel Proximity, el flujo de autenticación evita revelar si una cuenta existe o no, reduciendo el riesgo de enumeración de usuarios.

HORUS se configura para que la información sensible solo sea tratada en el contexto de una alerta, comunicación o servicio autorizado, conforme a la finalidad concreta para la que fue habilitado.

## 11. Registro, auditoría y trazabilidad

La plataforma mantiene logs de auditoría de actividad, eventos de sistema y transparencia de acceso, con retención de 400 días en el bucket _Required, configurado como bloqueado.

El resto de logs se conserva durante 180 días en el bucket _Default. Asimismo, los logs de aplicación se envían a Cloud Logging y los errores se monitorizan mediante Cloud Error Reporting.

Estas medidas permiten investigar incidencias, detectar usos indebidos, acreditar actuaciones y disponer de trazabilidad suficiente ante posibles reclamaciones, auditorías o requerimientos de autoridad competente.

## 12. Continuidad operativa y gestión de alertas

Para los procesos críticos de HORUS, el sistema utiliza Cloud Tasks y Cloud Scheduler para gestionar tareas asíncronas, reintentos y avisos no respondidos.

En particular, existe un proceso programado para reintentar avisos de alertas HORUS no atendidas, reforzando la disponibilidad del servicio en escenarios de emergencia.

## 13. Gestión de encargados y proveedores externos

SafeTroop identifica los proveedores externos que intervienen en el tratamiento, incluyendo Google Cloud, SMSPubli, Mailgun, Zoom Video SDK y Firebase.

Para dichos proveedores se prevé la existencia de contratos y acuerdos de tratamiento de datos, incluyendo acuerdos de encargo de tratamiento o DPA cuando corresponda.

En el caso de Zoom Video SDK, el tratamiento se limita a los elementos necesarios para la llamada HORUS, incluyendo token JWT firmado por el backend y transmisión de audio/vídeo entre usuario y agente autorizado.

## 14. Limitación de conservación y bloqueo ante reclamaciones

Los datos y evidencias generados por HORUS deberán conservarse únicamente durante los plazos definidos por SafeTroop o por el responsable del tratamiento, atendiendo a la finalidad del servicio, posibles obligaciones legales y eventuales reclamaciones.

En caso de incidencia, reclamación, investigación o requerimiento de autoridad competente, SafeTroop podrá aplicar medidas de bloqueo, exportación segura o conservación reforzada de la información afectada, restringiendo su acceso únicamente a personal autorizado y manteniendo la trazabilidad de las actuaciones realizadas.

## 15. Revisión periódica y mejora continua

Las medidas anteriores serán revisadas periódicamente y adaptadas en función de la evolución técnica de la plataforma, del resultado de las evaluaciones de riesgo, de las obligaciones aplicables al responsable del tratamiento y de las recomendaciones derivadas de auditorías de seguridad, RGPD o ENS.

Asimismo, SafeTroop mantendrá un proceso de mejora continua orientado a reforzar progresivamente los controles de acceso, cifrado, segregación de permisos, trazabilidad, conservación limitada de la información y gestión segura de evidencias digitales.

# 12. DERECHOS DEL INTERESADO

El usuario podrá ejercer en cualquier momento sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad, dirigiéndose a:

info@safetroop.com

Asimismo, podrá presentar reclamación ante la Agencia Española de Protección de Datos.

# 13. COLECTIVOS VULNERABLES

En los supuestos en los que el servicio HORUS sea utilizado por colectivos vulnerables o personas con capacidad limitada, el tratamiento de datos se realizará con especial atención a los principios de proporcionalidad, minimización y protección reforzada, sin perjuicio de las obligaciones legales que puedan corresponder a representantes legales o entidades colaboradoras.

# 14. MODIFICACIÓN DEL ANEXO

SafeTroop se reserva el derecho a modificar el presente Anexo para adaptarlo a cambios normativos, técnicos o funcionales del servicio HORUS, informando de ello conforme a la normativa vigente.

# REGISTRO DE ACTIVIDADES DE TRATAMIENTO

**SERVICIO HORUS – ALERTAS PERSONALES DE EMERGENCIA**

*(Artículo 30 RGPD)*

# 1. RESPONSABLE DEL TRATAMIENTO

**SAFETROOP TECHNOLOGIES, S.L.**
CIF: B44925204
Domicilio social: Carrer de L'Escorial 115, planta 5, puerta A, CP 08024, Barcelona (España)
Correo electrónico de contacto: info@safetroop.com

# 2. FINALIDAD DEL TRATAMIENTO

Gestión de situaciones de emergencia activadas voluntariamente por el usuario mediante el servicio HORUS, con las siguientes finalidades específicas:

- Recepción y gestión de alertas personales de emergencia.
- Localización inmediata del usuario durante situaciones de riesgo.
- Transmisión de información relevante a Fuerzas y Cuerpos de Seguridad, servicios de emergencia y autoridades competentes.
- Protección de la vida, integridad física y seguridad del usuario.

# 3. DESCRIPCIÓN DE LAS CATEGORÍAS DE INTERESADOS

- Usuarios registrados del servicio HORUS.
- Personas físicas que activan voluntariamente una alerta de emergencia.

# 4. CATEGORÍAS DE DATOS PERSONALES TRATADOS

- Datos identificativos: nombre y apellidos, dirección postal, número de teléfono, correo electrónico.
- Datos de localización: geolocalización en tiempo real durante la activación de la alerta.
- Datos de audio y vídeo: imágenes y sonido captados por la cámara y el micrófono del dispositivo del usuario.
- Datos técnicos: dirección IP, identificadores del dispositivo, datos de conexión y comunicación.

# 5. BASE JURÍDICA DEL TRATAMIENTO

- Consentimiento explícito del interesado (art. 6.1.a RGPD).
- Protección de intereses vitales del interesado o de otras personas físicas (art. 6.1.d RGPD).
- Misión realizada en interés público cuando intervienen autoridades competentes (art. 6.1.e RGPD).

## 6. CATEGORÍAS DE DESTINATARIOS

- Fuerzas y Cuerpos de Seguridad del Estado.
- Servicios de emergencia y protección civil.
- Autoridades judiciales o administrativas competentes.
- Proveedores tecnológicos que actúan como Encargados del Tratamiento conforme al artículo 28 RGPD.

## 7. TRANSFERENCIAS INTERNACIONALES DE DATOS

Podrán producirse transferencias internacionales de datos cuando los proveedores tecnológicos utilizados para la prestación del servicio se encuentren ubicados fuera del Espacio Económico Europeo, adoptándose en todo caso las garantías adecuadas conforme al RGPD, tales como cláusulas contractuales tipo o decisiones de adecuación de la Comisión Europea.

Las transferencias internacionales de datos personales que pudieran derivarse del uso de plataformas tecnológicas de terceros, como Zoom Video Communications, Inc., se realizan de conformidad con lo dispuesto en los artículos 44 y siguientes del Reglamento (UE) 2016/679 (RGPD), estando amparadas en las Cláusulas Contractuales Tipo aprobadas por la Comisión Europea y, en su caso, en la adhesión del proveedor al EU–US Data Privacy Framework, garantizando en todo momento un nivel de protección esencialmente equivalente al exigido en la Unión Europea.

## 8. PLAZO PREVISTO PARA LA SUPRESIÓN DE LOS DATOS

- Durante el tiempo estrictamente necesario para la gestión de la emergencia.
- Posteriormente, durante los plazos legales de conservación aplicables para la atención de responsabilidades legales.
- Finalizados dichos plazos, los datos serán bloqueados o suprimidos conforme a la normativa vigente.

## 9. DESCRIPCIÓN GENERAL DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD

- Activación manual y voluntaria del servicio por parte del usuario.
- Control de accesos restringido al personal autorizado.
- Cifrado de las comunicaciones cuando resulte técnicamente aplicable.
- Registro de accesos y trazabilidad de las operaciones.
- Medidas de privacidad desde el diseño y por defecto.

- Evaluación de riesgos del tratamiento.
- Procedimientos de gestión de brechas de seguridad y notificación a la autoridad de control.

## 10. OBSERVACIONES

El tratamiento de datos personales realizado a través del servicio HORUS presenta un nivel de riesgo elevado debido a la naturaleza de los datos tratados. SafeTroop ha adoptado medidas reforzadas de seguridad y ha evaluado los riesgos asociados conforme a los principios del Reglamento General de Protección de Datos.

# EVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS (EIPD / DPIA) – RESUMEN

**SERVICIO HORUS – ALERTAS PERSONALES DE EMERGENCIA**

*(Artículos 35 y 36 RGPD)*

## 1. IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

**SAFETROOP TECHNOLOGIES, S.L.**
CIF: B44925204
Domicilio social: Carrer de L'Escorial 115, planta 5, puerta A, CP 08024, Barcelona (España)
Correo electrónico de contacto: info@safetroop.com

## 2. DESCRIPCIÓN GENERAL DEL TRATAMIENTO

El servicio HORUS es una funcionalidad de alerta personal diseñada para situaciones de emergencia, que permite al usuario, mediante una activación voluntaria, consciente y expresa, transmitir una señal de auxilio desde su dispositivo móvil.

Dicha activación habilita temporalmente el tratamiento de determinados datos personales de carácter sensible, incluyendo datos de geolocalización en tiempo real y datos de audio y vídeo, con la finalidad exclusiva de gestionar la situación de emergencia y proteger los intereses vitales del usuario.

El tratamiento no se realiza de forma continua ni automática, quedando limitado estrictamente al tiempo de duración de la emergencia.

## 3. NECESIDAD Y PROPORCIONALIDAD DEL TRATAMIENTO

El tratamiento de datos personales realizado a través del servicio HORUS se considera necesario y proporcionado, dado que:

- La finalidad del servicio es la protección de la vida e integridad física del usuario.
- Los datos tratados son imprescindibles para permitir la localización y asistencia inmediata en situaciones de riesgo.
- El tratamiento se activa únicamente por decisión del usuario.
- Se aplican principios de minimización, limitación de finalidad y conservación restringida.

No existen medios alternativos menos intrusivos que permitan alcanzar con la misma eficacia la finalidad perseguida.

## 4. CATEGORÍAS DE DATOS Y DE INTERESADOS

**Categorías de datos:**

- Datos identificativos.
- Datos de localización en tiempo real.
- Datos de audio y vídeo.
- Datos técnicos del dispositivo.

**Categorías de interesados:**

- Usuarios registrados del servicio HORUS.
- Personas físicas que activan voluntariamente una alerta de emergencia.

## 5. IDENTIFICACIÓN DE LOS RIESGOS PARA LOS DERECHOS Y LIBERTADES

Se han identificado los siguientes riesgos principales:

- Acceso no autorizado a datos de geolocalización.
- Uso indebido de imágenes o grabaciones de audio.
- Divulgación accidental de datos personales.
- Tratamiento incidental de datos de terceros.
- Riesgo reputacional para los interesados en caso de brecha de seguridad.

## 6. MEDIDAS ADOPTADAS PARA MITIGAR LOS RIESGOS

Para reducir los riesgos identificados, SafeTroop ha implementado las siguientes medidas:

- Activación manual del servicio por parte del usuario.
- Limitación temporal estricta del tratamiento.

- Control de accesos y autenticación reforzada.
- Cifrado de las comunicaciones cuando sea técnicamente posible.
- Registro de accesos y trazabilidad de las operaciones.
- Formación específica del personal autorizado.
- Contratos de encargado del tratamiento conforme al artículo 28 RGPD.
- Procedimientos de gestión y notificación de brechas de seguridad.
- Aplicación de los principios de privacidad desde el diseño y por defecto.

## 7. EVALUACIÓN DEL RIESGO RESIDUAL

Tras la aplicación de las medidas técnicas y organizativas descritas, el nivel de riesgo residual para los derechos y libertades de los interesados se considera medio-bajo, teniendo en cuenta:

- La naturaleza excepcional del tratamiento.
- La activación voluntaria por parte del usuario.
- La finalidad de protección de intereses vitales.

No se aprecia la necesidad de consulta previa a la autoridad de control conforme al artículo 36 del RGPD.

## 8. PARTICIPACIÓN DE ENCARGADOS DEL TRATAMIENTO

Determinados proveedores tecnológicos participan en el tratamiento de datos en calidad de Encargados del Tratamiento, actuando bajo instrucciones documentadas de SafeTroop y con las garantías contractuales exigidas por el RGPD.

## 9. TRANSFERENCIAS INTERNACIONALES DE DATOS

En caso de que se produzcan transferencias internacionales de datos, se aplicarán las garantías adecuadas conforme a los artículos 44 y siguientes del RGPD.

## 10. CONCLUSIÓN DE LA EIPD

A la vista de la presente evaluación, se concluye que el tratamiento de datos personales realizado a través del servicio HORUS:

- Es conforme al Reglamento General de Protección de Datos.
- Es necesario y proporcionado a la finalidad perseguida.
- Incorpora medidas suficientes para mitigar los riesgos identificados.
- No requiere consulta previa a la Agencia Española de Protección de Datos en su versión resumida.

# 11. REVISIÓN Y ACTUALIZACIÓN

La presente EIPD resumida será revisada periódicamente y, en todo caso, cuando se produzcan cambios sustanciales en el servicio HORUS, en la normativa aplicable o en los riesgos asociados al tratamiento.