TRACTAMENT DE DADES PERSONALS DEL SERVEI HORUS

(ALERTES PERSONALS D'EMERGÈNCIA)

Annex a la Política de Privacitat de SAFETROOP TECHNOLOGIES, S.L.

El present Annex forma part integral de la Política de Privacitat general de SAFETROOP TECHNOLOGIES, S.L. i regula de manera específica el tractament de dades personals realitzat a través del servei HORUS, donada la naturalesa especialment sensible de les dades tractades i les finalitats d'emergència associades a dit servei.

1. DESCRIPCIÓ DEL SERVEI HORUS

HORUS és un servei d'alerta personal dissenyat per a la seva utilització en situacions d'emergència, risc o perill per a la integritat física de l'usuari. El servei permet, mitjançant una activació voluntària, expressa i conscient, l'enviament d'una senyal de socors que habilita determinades funcionalitats avançades del dispositiu mòbil de l'usuari amb la finalitat exclusiva de gestionar la situació d'emergència.

El servei HORUS no realitza cap tractament de dades de forma contínua, automàtica ni passiva, quedant totes les seves funcionalitats avançades desactivades per defecte fins a l'activació expressa per part de l'usuari.

2. RESPONSABLE DEL TRACTAMENT

El responsable del tractament de les dades personals tractades a través del servei HORUS és:

SAFETROOP TECHNOLOGIES, S.L.
CIF: B44925204
Domicili social: Carrer de L'Escorial 115, planta 5, porta A, CP 08024, Barcelona (Espanya)
Correu electrònic de contacte: info@safetroop.com

3. CATEGORIES DE DADES PERSONALS TRACTADES

Exclusivament en el moment en què l'usuari activa manualment una alerta HORUS, podran tractarse les següents categories de dades personals:

a) Dades identificatives

- Nom i cognoms
- Adreça postal
- Número de telèfon
- Adreça de correu electrònic

b) Dades de localització

- Dades de geolocalització en temps real del dispositiu de l'usuari durant l'activació de l'alerta.

c) Dades d'àudio i vídeo

- Imatges i so captats per la càmera i el micròfon del dispositiu de l'usuari durant la gestió de l'emergència.

d) Dades tècniques

- Adreça IP
- Identificadors del dispositiu
- Informació tècnica necessària per a la transmissió de l'alerta i la comunicació amb els serveis d'emergència.

4. FINALITAT ESPECÍFICA DEL TRACTAMENT

Les dades personals tractades a través del servei HORUS s'utilitzaran exclusivament per a les següents finalitats:

- Gestionar i atendre situacions d'emergència comunicades per l'usuari.
- Permetre la localització immediata de l'usuari durant una situació de risc.
- Facilitar la intervenció de Forces i Cossos de Seguretat, serveis d'emergència, protecció civil o altres autoritats competents.
- Protegir la vida, integritat física i seguretat de l'usuari.

Les dades no seran utilitzades per a finalitats comercials, publicitàries ni analítiques.

5. BASE JURÍDICA DEL TRACTAMENT

El tractament de dades personals en el servei HORUS es legitima conforme al disposat en l'article 6 del RGPD, en base a:

- El consentiment explícit de l'usuari (art. 6.1.a RGPD), manifestat mitjançant l'activació conscient del sistema d'alerta.
- La protecció d'interessos vitals de l'interessat o d'altres persones físiques (art. 6.1.d RGPD).

- Quan resulti aplicable, el compliment d'una missió realitzada en interès públic per part de les autoritats intervinents (art. 6.1.e RGPD).

6. ACTIVACIÓ DEL SERVEI I CONTROL DE L'USUARI

L'activació del tractament de dades en HORUS:

- Es produeix únicament mitjançant una acció voluntària de l'usuari.
- No s'activa per la mera utilització o instal·lació de l'aplicació.
- Pot ser finalitzada per l'usuari en qualsevol moment, sense perjudici de les obligacions legals de conservació que puguin resultar aplicables.

7. TRACTAMENT INCIDENTAL DE DADES DE TERCERS

Durant l'activació d'una alerta HORUS, poden captarse de forma incidental imatges o sons de terceres persones que es trobin en l'entorn de l'usuari. Dit tractament:

- Es considera estrictament accessori i necessari per a la gestió de l'emergència.
- Es limita a la finalitat de protecció d'interessos vitals.
- No serà objecte d'usos addicionals ni independents.

8. DESTINATARIS DE LES DADES

Les dades personals tractades a través de HORUS podran ser comunicades, quan resulti estrictament necessari, a:

- Forces i Cossos de Seguretat de l'Estat.
- Serveis d'emergència i protecció civil.
- Autoritats judicials o administratives competents.

Així mateix, determinats proveïdors tecnològics podran accedir a les dades en qualitat d'Encarregats del Tractament, conforme a contractes subscrits d'acord amb l'article 28 del RGPD.

9. VIDEOCOMUNICACIONS I ÚS DE PLATAFORMES DE TERCERS

Les comunicacions d'àudio i vídeo del servei HORUS es realitzen mitjançant plataformes tecnològiques de tercers, com Zoom Video Communications, Inc., que actuen com Encarregats del Tractament, en conformitat amb els seus respectius acuerdos de tractament de dades (DPA) i amb les garanties exigides pel RGPD.

SafeTroop manté en tot cas la condició de Responsable del Tractament.

10. TERMINI DE CONSERVACIÓ DE LES DADES

Les dades personals generades durant una alerta HORUS es conservaran:

- Durant el temps estrictament necessari per a la gestió de l'emergència.
- Posteriorment, durant els terminis legals de prescripció aplicables per a l'atenció de possibles responsabilitats legals.
- Transcorreguts dits terminis, les dades seran bloquejades o suprimides conforme a la normativa vigent.

11. MESURES DE SEGURETAT I PRIVACITAT DES DEL DISSENY

Donada la naturalesa especialment sensible del tractament associat a HORUS, que pot incloure dades identificatives, dades de localització en temps real, àudio, vídeo, informació sobre situacions d'emergència i dades vinculades a col·lectius vulnerables, SafeTroop ha implementat mesures tècniques i organitzatives orientades a garantir la confidencialitat, integritat, disponibilitat, trazabilitat i minimització del tractament.

En particular, s'apliquen les següents mesures:

1. Allotjament de la informació en entorn europeu

La plataforma es troba desplegada sobre Google Cloud Platform a la regió europe-west1, Bèlgica, mantenint els principals serveis de tractament dins de l'Espai Econòmic Europeu. Els buckets d'emmagatzematge es troben igualment configurats en entorn EU, reduint el risc de transferències internacionals no controlades.

2. Arquitectura segregada i reducció de superfície d'exposició

La solució s'organitza en components diferenciats per backend, panells d'administració i aplicacions mòbils. El backend exposa diferents esquemes GraphQL separats per a Connectpol, Proximity i Proximity/HORUS, cadascun amb la seva pròpia clau d'API.

Els serveis Cloud Run es troben configurats amb accés internal-and-cloud-load-balancing, evitant la seva exposició directa a Internet i canalitzant l'accés a través del balanceador segur.

3. Protecció perimetral i control del tràfic

L'accés públic es realitza mitjançant un Google Cloud Load Balancer amb certificats SSL gestionats i política de seguretat Cloud Armor, incloent limitació de tràfic per IP i bloqueig automàtic quan se superen els llindar definits. Aquesta mesura contribueix a mitigar abusos, automatismes, atacs de força bruta i tràfic anòmal.

4. Xifratge de les comunicacions

Les comunicacions externes es realitzen mitjançant HTTPS amb TLS 1.2 o superior. La política SSL aplicada deshabilita suites criptogràfiques dèbils o basades en intercanvi RSA estàtic, prioritzant suites ECDHE amb forward secrecy.

Les comunicacions internes entre Cloud Run, Cloud SQL, Cloud Storage, Secret Manager, Datastream i BigQuery es realitzen mitjançant canals xifratsgestats per Google Cloud.

5. Seguretat de la base de dades i emmagatzematge

L'accés del backend a Cloud SQL es realitza mitjançant Cloud SQL Auth Proxy, executat com sidecar dins del mateix entorn Cloud Run. L'aplicació es connecta al proxy per socket Unix local, evitant l'exposició directa de la base de dades a la xarxa.

L'accés extern a Cloud SQL queda restringit a xarxes autoritzades i a les IPs estàtiques de sortida definides per a Cloud Run i el pipeline CI.

Les dades en repòs es troben xifrandes mitjançant xifratge gestionat per Google. A més, Cloud SQL disposa de còpies de seguretat diàries i binary log activat.

6. Separació entre informació privada i pública

El sistema diferencia entre buckets d'emmagatzematge privats i públics. El bucket privat s'utilitza per a fitxers interns, informes i adjunts, mentre que el bucket públic queda limitat a imatges i actius públics. Aquesta separació redueix el risc d'exposició accidental de documentació sensible.

7. Gestió segura de secrets i credencials

Les claus sensibles, incloent la clau privada RSA utilitzada per a la firma de JWT, es custodien en Google Secret Manager.

L'accés programàtic es realitza mitjançant comptes de servei específics i restringits, utilitzats des de Cloud Run i des del pipeline de desplegament corresponent. Les credencials d'accés queden limitades a usuaris autoritzats i al procés d'integració contínua.

8. Autenticació reforcida i control de sessions

L'accés a la plataforma es realitza mitjançant fluxos d'autenticació basats en codis OTP enviats per SMS o correu electrònic, amb codis de 6 dígits, caducitat limitada a 3 minuts i nombre màxim d'intents.

Un cop validat l'accés, el sistema emet tokens JWT signats amb RS256 i expiració curta, juntament amb refresh tokens d'alta entropia. Aquesta configuració limita l'impacte d'una eventual exposició de credencials o tokens.

9. Control d'autorització per rols i claus API

Tota petició GraphQL requereix una clau X-Api-Key específica de l'esquema corresponent i, excepte els endpoints d'autenticació, un token Bearer JWT vàlid.

El sistema aplica autorització mitjançant rols diferenciats, incloent perfils com ADMIN, MANAGER, USER, PROXIMITY_MANAGER i GUEST. Les directrius d'autorització validen tant l'autenticació com els permisos necessaris per a cada operació.

10. Principi de minimització i privacitat per defecte

El sistema limita l'accés a la informació a usuaris autenticats i autoritzats segons el seu rol, evitant accesos generalitzats o innecessaris a dades personals o informació sensible.

En el cas del panell Proximity, el flux d'autenticació evita revelar si un compte existeix o no, reduint el risc d'enumeració d'usuaris.

HORUS es configura per a que la informació sensible només sigui tractada en el context d'una alerta, comunicació o servei autoritzat, conforme a la finalitat concreta per a la qual fou habilitat.

11. Registre, auditoria i trazabilitat

La plataforma manté logs d'auditoria d'activitat, eventos de sistema i transparència d'accés, amb retención de 400 dies en el bucket _Required, configurat com bloqueado.

La resta de logs es conserva durant 180 dies en el bucket _Default. Així mateix, els logs d'aplicació s'envien a Cloud Logging i els errors es monitorizan mitjançant Cloud Error Reporting.

Aquestes mesures permeten investigar incidències, detectar usos indeguts, acreditar actuacions i disposar de trazabilitat suficient davant de possibles reclamacions, auditories o requeriments d'autoritat competent.

12. Continuïtat operativa i gestió d'alertes

Per als processos crítics de HORUS, el sistema utilitza Cloud Tasks i Cloud Scheduler per a gestionar tasques asíncrones, reintentos i avisos no respondits.

En particular, existeix un procés programat per a reintentar avisos d'alertes HORUS no ateses, reforcint la disponibilitat del servei en escenaris d'emergència.

13. Gestió d'encarregats i proveïdors externs

SafeTroop identifica els proveïdors externs que intervenen en el tractament, incloent Google Cloud, SMSPubli, Mailgun, Zoom Video SDK i Firebase.

Per a dits proveïdors es preveu l'existència de contractes i acuerdos de tractament de dades, incloent acuerdos d'encàrrec de tractament o DPA quan correspongui.

En el cas de Zoom Video SDK, el tractament es limita als elements necessaris per a la trucada HORUS, incloent token JWT signat pel backend i transmissió d'àudio/vídeo entre usuari i agent autoritzat.

14. Limitació de conservació i bloqueig davant de reclamacions

Les dades i evidències generades per HORUS hauran de conservarse únicament durant els terminis definits per SafeTroop o pel responsable del tractament, atenent a la finalitat del servei, possibles obligacions legals i eventualment reclamacions.

En cas d'incidència, reclamació, investigació o requeriment d'autoritat competent, SafeTroop podrà aplicar mesures de bloqueig, exportació segura o conservació reforcida de la informació afectada, restringint el seu accés únicament a personal autoritzat i mantenint la trazabilitat de les actuacions realitzades.

15. Revisió periòdica i millora contínua

Les mesures anteriors seran revisades periòdicament i adaptades en funció de l'evolució tècnica de la plataforma, del resultat de les avaluacions de risc, de les obligacions aplicables al responsable del tractament i de les recomanacions derivades d'auditories de seguretat, RGPD o ENS.

Així mateix, SafeTroop mantindrà un procés de millora contínua orientat a reforcir progressivament els controls d'accés, xifratge, segregació de permisos, trazabilitat, conservació limitada de la informació i gestió segura d'evidències digitals.

12. DRETS DE L'INTERESSAT

L'usuari podrà exercir en qualsevol moment els seus drets d'accés, rectificació, supressió, oposició, limitació del tractament i portabilitat, dirigint-se a:

info@safetroop.com

Així mateix, podrà presentar reclamació davant de l'Autoritat Catalana de Protecció de Dades.

13. COL·LECTIUS VULNERABLES

En els supòsits en els quals el servei HORUS sigui utilitzat per col·lectius vulnerables o persones amb capacitat limitada, el tractament de dades es realitzarà amb especial atenció als principis de proporcionalitat, minimització i protecció reforcida, sense perjudici de les obligacions legals que puguin correspondre a representants legals o entitats col·laboradores.

14. MODIFICACIÓ DE L'ANNEX

SafeTroop es reserva el dret de modificar el present Annex per a adaptar-lo a canvis normatius, tècnics o funcionals del servei HORUS, informant de tot plegat conforme a la normativa vigent.

REGISTRE D'ACTIVITATS DE TRACTAMENT

SERVEI HORUS – ALERTES PERSONALS D'EMERGÈNCIA

(Article 30 RGPD)

1. RESPONSABLE DEL TRACTAMENT

SAFETROOP TECHNOLOGIES, S.L.
CIF: B44925204
Domicili social: Carrer de L'Escorial 115, planta 5, porta A, CP 08024, Barcelona (Espanya)
Correu electrònic de contacte: info@safetroop.com

2. FINALITAT DEL TRACTAMENT

Gestió de situacions d'emergència activades voluntàriament per l'usuari mitjançant el servei HORUS, amb les següents finalitats específiques:

- Recepció i gestió d'alertes personals d'emergència.
- Localització immediata de l'usuari durant situacions de risc.
- Transmissió d'informació rellevant a Forces i Cossos de Seguretat, serveis d'emergència i autoritats competents.
- Protecció de la vida, integritat física i seguretat de l'usuari.

3. DESCRIPCIÓ DE LES CATEGORIES D'INTERESSATS

- Usuaris registrats del servei HORUS.
- Persones físiques que activen voluntàriament una alerta d'emergència.

4. CATEGORIES DE DADES PERSONALS TRACTADES

- Dades identificatives: nom i cognoms, adreça postal, número de telèfon, correu electrònic.
- Dades de localització: geolocalització en temps real durant l'activació de l'alerta.
- Dades d'àudio i vídeo: imatges i so captats per la càmera i el micròfon del dispositiu de l'usuari.
- Dades tècniques: adreça IP, identificadors del dispositiu, dades de connexió i comunicació.

5. BASE JURÍDICA DEL TRACTAMENT

- Consentiment explícit de l'interessat (art. 6.1.a RGPD).
- Protecció d'interessos vitals de l'interessat o d'altres persones físiques (art. 6.1.d RGPD).
- Missió realitzada en interès públic quan intervenen autoritats competents (art. 6.1.e RGPD).

6. CATEGORIES DE DESTINATARIS

- Forces i Cossos de Seguretat de l'Estat.
- Serveis d'emergència i protecció civil.
- Autoritats judicials o administratives competents.
- Proveïdors tecnològics que actuen com Encarregats del Tractament conforme a l'article 28 RGPD.

7. TRANSFERÈNCIES INTERNACIONALS DE DADES

Podran produir-se transferències internacionals de dades quan els proveïdors tecnològics utilitzats per a la prestació del servei es trobin ubicats fora de l'Espai Econòmic Europeu, adoptant-se en tot cas les garanties adequades conforme al RGPD, com cláusules contractuals tipus o decisions d'adecuació de la Comissió Europea.

Les transferències internacionals de dades personals que poguessin derivar-se del ús de plataformes tecnològiques de tercers, com Zoom Video Communications, Inc., es realitzen en conformitat amb el disposat en els articles 44 i següents del Reglament (UE) 2016/679 (RGPD), estant amparades en les Cláusules Contractuals Tipus aprovades per la Comissió Europea i, en el seu cas, en l'adhesió del proveïdor al EU–US Data Privacy Framework, garantint en tot moment un nivell de protecció essencialment equivalent al exigit en la Unió Europea.

8. TERMINI PREVIST PER A LA SUPRESSIÓ DE LES DADES

- Durant el temps estrictament necessari per a la gestió de l'emergència.
- Posteriorment, durant els terminis legals de conservació aplicables per a l'atenció de responsabilitats legals.
- Finalitzats dits terminis, les dades seran bloquejades o suprimides conforme a la normativa vigent.

9. DESCRIPCIÓ GENERAL DE LES MESURES TÈCNIQUES I ORGANITZATIVES DE SEGURETAT

- Activació manual i voluntària del servei per part de l'usuari.
- Control d'accés restringit al personal autoritzat.
- Xifratge de les comunicacions quan resulti tècnicament aplicable.
- Registre d'accés i trazabilitat de les operacions.
- Mesures de privacitat des del disseny i per defecte.
- Avaluació de riscos del tractament.
- Procediments de gestió de breques de seguretat i notificació a l'autoritat de control.

10. OBSERVACIONS

El tractament de dades personals realitzat a través del servei HORUS presenta un nivell de risc elevat degut a la naturalesa de les dades tractades. SafeTroop ha adoptat mesures reforcides de seguretat i ha avaluat els riscos associats conforme als principis del Reglament General de Protecció de Dades.

AVALUACIÓ D'IMPACTE EN PROTECCIÓ DE DADES (AIPD / DPIA) – RESUM

SERVEI HORUS – ALERTES PERSONALS D'EMERGÈNCIA

(Articles 35 i 36 RGPD)

1. IDENTIFICACIÓ DEL RESPONSABLE DEL TRACTAMENT

SAFETROOP TECHNOLOGIES, S.L.
CIF: B44925204
Domicili social: Carrer de L'Escorial 115, planta 5, porta A, CP 08024, Barcelona (Espanya)
Correu electrònic de contacte: info@safetroop.com

2. DESCRIPCIÓ GENERAL DEL TRACTAMENT

El servei HORUS és una funcionalitat d'alerta personal dissenyada per a situacions d'emergència, que permet a l'usuari, mitjançant una activació voluntària, conscient i expressa, transmetre una senyal de socors des del seu dispositiu mòbil.

Dita activació habilita temporalment el tractament de determinades dades personals de caràcter sensible, incloent dades de geolocalització en temps real i dades d'àudio i vídeo, amb la finalitat exclusiva de gestionar la situació d'emergència i protegir els interessos vitals de l'usuari.

El tractament no es realitza de forma contínua ni automàtica, quedant limitat estrictament al temps de durada de l'emergència.

3. NECESSITAT I PROPORCIONALITAT DEL TRACTAMENT

El tractament de dades personals realitzat a través del servei HORUS es considera necessari i proporcionat, atès que:

- La finalitat del servei és la protecció de la vida i integritat física de l'usuari.
- Les dades tractades són imprescindibles per a permetre la localització i assistència immediata en situacions de risc.
- El tractament s'activa únicament per decisió de l'usuari.
- S'apliquen principis de minimització, limitació de finalitat i conservació restringida.

No existeixen mitjans alternatius menys intrusos que permetin assolir amb la mateixa eficàcia la finalitat perseguida.

4. CATEGORIES DE DADES I D'INTERESSATS

Categories de dades:

- Dades identificatives.
- Dades de localització en temps real.
- Dades d'àudio i vídeo.
- Dades tècniques del dispositiu.

Categories d'interessats:

- Usuaris registrats del servei HORUS.
- Persones físiques que activen voluntàriament una alerta d'emergència.

5. IDENTIFICACIÓ DELS RISCOS PER ALS DRETS I LLIBERTATS

S'han identificat els següents riscos principals:

- Accés no autoritzat a dades de geolocalització.
- Ús indegut d'imatges o gravacions d'àudio.
- Divulgació accidental de dades personals.
- Tractament incidental de dades de tercers.
- Risc reputacional per als interessats en cas de brecha de seguretat.

6. MESURES ADOPTADES PER MITIGAR ELS RISCOS

Per a reduir els riscos identificats, SafeTroop ha implementat les següents mesures:

- Activació manual del servei per part de l'usuari.
- Limitació temporal estricta del tractament.
- Control d'accés i autenticació reforcida.
- Xifratge de les comunicacions quan sigui tècnicament possible.
- Registre d'accés i trazabilitat de les operacions.
- Formació específica del personal autoritzat.
- Contractes d'encarregat del tractament conforme a l'article 28 RGPD.

- Procediments de gestió i notificació de breques de seguretat.
- Aplicació dels principis de privacitat des del disseny i per defecte.

7. AVALUACIÓ DEL RISC RESIDUAL

Després de l'aplicació de les mesures tècniques i organitzatives descrites, el nivell de risc residual per als drets i llibertats dels interessats es considera mitjà-baix, tenint en compte:

- La naturalesa excepcional del tractament.
- L'activació voluntària per part de l'usuari.
- La finalitat de protecció d'interessos vitals.

No s'aprecia la necessitat de consulta prèvia a l'autoritat de control conforme a l'article 36 del RGPD.

8. PARTICIPACIÓ D'ENCARREGATS DEL TRACTAMENT

Determinats proveïdors tecnològics participen en el tractament de dades en qualitat d'Encarregats del Tractament, actuant sota instruccions documentades de SafeTroop i amb les garanties contractuals exigides pel RGPD.

9. TRANSFERÈNCIES INTERNACIONALS DE DADES

En cas que es produïxin transferències internacionals de dades, s'aplicaran les garanties adequades conforme als articles 44 i següents del RGPD.

10. CONCLUSIÓ DE L'AIPD

A la vista de la present avaluació, es conclou que el tractament de dades personals realitzat a través del servei HORUS:

- És conforme al Reglament General de Protecció de Dades.
- És necessari i proporcionat a la finalitat perseguida.
- Incorpora mesures suficients per a mitigar els riscos identificats.
- No requereix consulta prèvia a l'Autoritat Catalana de Protecció de Dades en la seva versió resumida.

11. REVISIÓ I ACTUALITZACIÓ

La present AIPD resumida serà revisada periòdicament i, en tot cas, quan es produeixin canvis substancials en el servei HORUS, en la normativa aplicable o en els riscos associats al tractament.