REGISTRE D'ACTIVITATS I CATEGORIES D'ACTIVITATS DE TRACTAMENT

Reglament General de Protecció de Dades (UE) 2016/679
Llei orgànica 3/2018, de protecció de dades personals
i garantia dels drets digitals

Safetroop Technologies, S.L.

Dades del Responsable

SAFETROOP TECHNOLOGIES S.L.
B44925204
C/ Carrer Espinoi 8/10 Local 1
08024 - Barcelona
BARCELONA
ESPANYA

Dades de Contacte

Telèfon: +34 685378085
Email: info@safetroop.com

Delegat de Protecció de Dades

CARLOS TORTAJADA MONTUENGA
ADVOCAT ICAM 92637
Auditor RGPD
C. SANTA ENGRACIA, 17 - 6a PLANTA
28010 - MADRID
MADRID
ESPANYA
Tfno. 914456569
Email: equaldpo@equalprotecciondedatos.com

TRACTAMENTS DE DADES PERSONALS

1. INTRODUCCIÓ

El present document integra el Registre d'Activitats de Tractament efectuades per Safetroop Technologies, S.L. en qualitat de Responsable del Tractament, així com el Registre de Categories d'Activitats realitzades en qualitat d'Encarregat del Tractament, atès que actua en determinats tractaments com a Responsable del Tractament i, en altres, com a Encarregat del Tractament per compte d'Administracions Públiques, tot això de conformitat amb l'article 30 del Reglament (UE) 2016/679 (RGPD).

Així mateix, el present Registre es troba alineat amb el sistema de gestió de seguretat implantat per l'entitat i amb els requisits derivats de l'Esquema Nacional de Seguretat (ENS), constituint una eina de govern de la dada, traçabilitat i gestió de riscos.

Les mesures de seguretat reflectides en aquest document tenen caràcter informatiu i complementari a les evidències, polítiques, procediments i controls específics documentats en la Declaració d'Aplicabilitat (SoA), l'anàlisi de riscos i la resta de documentació ENS de l'entitat.

1.1. MESURES DE SEGURETAT GENERALS APLICABLES A TOTS ELS TRACTAMENTS

SAFETROOP TECHNOLOGIES, S.L. disposa d'un sistema de gestió de seguretat de la informació alineat amb l'Esquema Nacional de Seguretat (ENS), que incorpora mesures organitzatives, operatives i tècniques destinades a garantir la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de la informació tractada.

Sense perjudici de les mesures que de forma extensa estan contemplades i auditades en els procediments de certificació de l'ENS, les mesures fonamentals que s'apliquen a tots els tractaments anteriors són les següents:

a) Govern i organització de la seguretat

El Responsable del Tractament disposa de:

- Política de Seguretat de la Informació formalment aprovada.
- Procediments de seguretat documentats.
- Sistema de gestió de riscos.
- Inventari d'actius.
- Processos de revisió i millora contínua.
- Gestió documental d'evidències de compliment.

b) Gestió d'identitats i control d'accessos

S'apliquen mesures destinades a garantir que únicament accedeixin a la informació les persones autoritzades, incloent-hi:

- Identificació individual d'usuaris.
- Autenticació robusta.
- Gestió formal d'altes, modificacions i baixes.
- Segregació de funcions.
- Principi de mínim privilegi.
- Revisió periòdica de permisos.

c) Protecció de sistemes i serveis

El Responsable del Tractament disposa de:

- Configuració segura de sistemes.
- Gestió de vulnerabilitats.
- Actualització i aplicació de pedaços.
- Protecció davant de codi maliciós.
- Control de canvis.
- Inventari d'actius tecnològics.

d) Registre d'activitat i traçabilitat

Es mantenen mecanismes de:

- Registre d'accessos.
- Registre d'activitat.

- Conservació d'evidències.
- Monitorització d'esdeveniments.
- Investigació d'incidents.
- Traçabilitat d'actuacions.

e) Protecció criptogràfica

La informació es protegeix mitjançant:

- Xifratge de comunicacions.
- Protecció de claus criptogràfiques.
- Protocols segurs de transmissió.
- Mesures de protecció de la informació emmagatzemada.

f) Seguretat de proveïdors i serveis cloud

El Responsable del Tractament manté procediments d'avaluació i supervisió de proveïdors, incloent-hi:

- Contractes d'encàrrec del tractament.
- Acords de nivell de servei.
- Avaluació de garanties de seguretat.
- Control d'interconnexions.
- Supervisió i avaluació contínua de proveïdors crítics.

g) Continuïtat i recuperació

Es disposa de:

- Còpies de seguretat periòdiques.
- Procediments de restauració.
- Mesures de continuïtat de negoci.
- Procediments de recuperació davant d'incidents.

2.2. Criteris generals de conservació de dades

Sense perjudici dels terminis de conservació que de forma específica sigui necessari contemplar en supòsits de tractaments concrets, amb caràcter general, les dades personals es conservaran durant el temps estrictament necessari per complir la finalitat per a la qual van ser recollides.

Un cop finalitzada aquesta finalitat, les dades podran romandre bloquejades durant els terminis legalment exigibles per atendre possibles responsabilitats administratives, tributàries, mercantils, civils, laborals o derivades de la normativa de protecció de dades i seguretat de la informació.

El bloqueig de dades es realitzarà de conformitat amb l'article 32 de la Llei orgànica 3/2018, de protecció de dades personals i garantia dels drets digitals.

Finalitzats els terminis de conservació i bloqueig aplicables, les dades seran suprimides o anonimitzades de forma segura.

Tractament	Conservació activa	Bloqueig / conservació posterior	Base jurídica i normativa
Clients	Durant la vigència de la relació contractual	Fins a 6 anys (mercantil), 4 anys (fiscal) i 5 anys per a accions contractuals	Art. 30 Codi de Comerç; arts. 66 a 70 Llei General Tributària; art. 1964 Codi Civil
Contactes web i sol·licituds d'informació	Fins a la resolució de la consulta o sol·licitud	Fins al termini de prescripció de possibles reclamacions	Art. 1964 Codi Civil; art. 32 LOPDGDD
Comptabilitat	Durant la gestió econòmica i fiscal	6 anys des de l'últim assentament comptable i, si escau, 4 anys a efectes tributaris	Art. 30 Codi de Comerç; Llei General Tributària
Proveïdors	Durant la vigència de la relació contractual	6 anys mercantil, 4 anys fiscal i 5 anys contractual	Art. 30 Codi de Comerç; arts. 66 a 70 Llei General Tributària; art. 1964 Codi Civil
Usuaris agents autoritzats	Durant la vigència del servei contractat per l'entitat responsable	Conforme a les instruccions documentades del Responsable del Tractament i a les	Art. 28 RGPD; contracte d'encàrrec del tractament

Tractament	Conservació activa	Bloqueig / conservació posterior	Base jurídica i normativa
		obligacions derivades del contracte d'encàrrec	
Alertes i incidències operatives	Durant la prestació del servei	Mentre sigui necessari per garantir traçabilitat, auditoria, investigació d'incidents o defensa jurídica	ENS; art. 32 RGPD; art. 32 LOPDGDD
Administració tècnica i suport	Durant la prestació del servei	Mentre sigui necessari per acreditar actuacions tècniques, incidències o responsabilitats derivades del suport prestat	Art. 1964 Codi Civil; ENS
Logs d'accés i seguretat	Conforme a la política de gestió de logs i seguretat de la informació	Mentre sigui necessari per a auditories, investigació d'incidents, compliment ENS i defensa jurídica	ENS; art. 32 RGPD; art. 32 LOPDGDD
Monitorització i esdeveniments de seguretat	Conforme a la política de monitorització i seguretat	Mentre sigui necessari per a investigació i traçabilitat d'incidents	ENS; Seguretat de la Informació
Còpies de seguretat	Segons la política de backup i continuïtat	Conforme als cicles de rotació definits i fins a la destrucció segura dels suports	ENS; Pla de Continuïtat i Recuperació
Registres relacionats amb incidents de seguretat	Durant la gestió activa de l'incident	Fins a la prescripció de possibles responsabilitats administratives, civils o contractuals	RGPD; LOPDGDD; Codi Civil

Conservació derivada de la normativa de protecció de dades

En aquells supòsits en què puguin derivar-se responsabilitats per incompliment de la normativa de protecció de dades, l'organització podrà conservar determinada informació bloquejada durant els terminis necessaris per atendre possibles procediments administratius, reclamacions o actuacions de l'autoritat de control competent.

A aquests efectes es tindran en consideració, entre altres disposicions:

- Reglament (UE) 2016/679 (RGPD).
- Llei orgànica 3/2018, de protecció de dades personals i garantia dels drets digitals.
- Llei 39/2015, del procediment administratiu comú de les administracions públiques.
- Llei 40/2015, de règim jurídic del sector públic.

Conservació d'evidències de seguretat i compliment ENS

Els registres, evidències, logs, traces, auditories i altra informació necessària per garantir la seguretat, traçabilitat, investigació d'incidents i compliment de l'Esquema Nacional de Seguretat podran conservar-se durant els terminis necessaris per:

- La investigació d'incidents de seguretat.
- La realització d'auditories internes o externes.
- L'acreditació del compliment normatiu.
- La defensa jurídica de l'organització.
- L'atenció de requeriments d'organismes públics competents.

La conservació d'aquestes evidències es realitzarà aplicant mesures adequades d'accés restringit, integritat, traçabilitat i protecció davant d'alteració o destrucció no autoritzada.

Supressió definitiva

Un cop transcorreguts els terminis de conservació i bloqueig indicats, les dades personals seran eliminades de forma segura o anonimitzades, aplicant procediments que impedeixin la seva recuperació posterior, llevat que existeixi una obligació legal específica que en justifiqui el manteniment.

ACTIVITATS COM A RESPONSABLE DEL TRACTAMENT

1.- CLIENTS

Finalitat del Tractament

La finalitat és la gestió de la relació mercantil, tant des d'un punt de vista administratiu i de compliment d'obligacions fiscals, com des d'un punt de vista comercial i de màrqueting.

Base jurídica de legitimació

El tractament de dades de contacte i, si escau, les relatives a la funció o lloc exercit per les persones físiques que prestin serveis en una persona jurídica (clients o proveïdors) estarà legitimat sobre la base jurídica de l'article 6.1.f) del RGPD, és a dir, l'interès legítim del Responsable del Tractament. D'acord amb l'article 19.1.a) de la LOPD 3/2018 únicament seran tractades les dades personals necessàries per a la localització professional. D'altra banda, per als clients considerats persones físiques o usuaris domèstics, el tractament de les seves dades està legitimat pels articles 6.1.b i 6.1.c, és a dir, l'execució d'un contracte i el compliment d'obligacions legals.

Termini de conservació

Un cop finalitzada la relació contractual o prestació de servei, les dades es conservaran bloquejades exclusivament per atendre possibles responsabilitats legals durant els terminis següents:

- 6 anys: article 30 del Codi de Comerç.
- 4 anys: articles 66 a 70 de la Llei General Tributària.
- 5 anys: article 1964 del Codi Civil.

Categories d'interessats

Clients i persones de contacte.

Categories de dades personals

Dades identificatives, professionals, dades de contacte, facturació i relació contractual.

Categories de destinataris de cessions

Administració tributària, altres òrgans de l'administració pública i bancs.

Encarregats de tractament

DRIBBA DEVELOPMENT & CONSULTING SOCIEDAD LIMITADA, empresa amb la qual es manté subscrit un contracte d'Encarregat del Tractament amb els requisits contemplats a l'article 28 del RGPD.

Transferències internacionals de dades

No es realitzen transferències internacionals.

Mesures de seguretat

Sense perjudici de les mesures generals de conformitat amb la certificació de l'ENS indicades a l'inici del present document, d'acord amb l'article 32 del RGPD 679/2016 el responsable ha realitzat una avaluació dels riscos des del punt de vista RGPD per poder garantir els drets de les persones interessades. Sobre la base d'aquesta avaluació s'han adoptat les mesures tècniques i organitzatives necessàries, que s'han reflectit en l'informe d'anàlisi de riscos corresponent.

MESURES PER A LA PSEUDONIMITZACIÓ I EL XIFRATGE:

S'utilitzaran contrasenyes úniques i intransferibles per accedir a les dades, que no podran ser revelades a terceres persones, ni tan sols a companys de feina:

- Generació i distribució de contrasenyes

La generació de contrasenyes la realitza l'administrador del sistema, que les comunica a l'usuari que les utilitzarà.

Els sistemes que realitzin la identificació de l'usuari garantiran que la introducció de la contrasenya i la seva representació en pantalla, en el moment de l'autenticació, s'efectuen en un format no llegible per a la resta d'usuaris.

- Emmagatzematge de les contrasenyes

No està permès als usuaris anotar els identificadors i contrasenyes, ni en paper ni en suport electrònic.

- Renovació periòdica de contrasenyes

Les contrasenyes són renovades pel mateix usuari que les utilitzarà, almenys una vegada a l'any i, a més, sempre que se sospiti que la seva confidencialitat ha pogut quedar compromesa.

MESURES PER RESTAURAR LA DISPONIBILITAT I L'ACCÉS A LES DADES DESPRÉS D'UN INCIDENT:

- Còpies de seguretat

Les còpies de seguretat es realitzen diàriament en els servidors de DRIBBA DEVELOPMENT & CONSULTING SOCIEDAD LIMITADA, empresa amb la qual es manté subscrit un contracte d'Encarregat del Tractament amb els requisits contemplats a l'article 28 del RGPD. La recuperació de dades des de les còpies de seguretat s'efectuarà per l'encarregat del tractament, o amb la seva autorització i sota la seva supervisió, sempre que es produeixi una alteració, pèrdua o destrucció, total o parcial, de les dades personals, havent-se de reconstruir l'estat en què es trobaven abans de la incidència.

Quan els fitxers o tractaments afectats per la incidència estiguin parcialment automatitzats i l'existència de documentació en paper permeti la reconstrucció òptima de les dades, aquestes s'hauran d'introduir manualment i deixar constància motivada d'aquesta actuació en la descripció de la incidència.

2.- PROVEÏDORS

Finalitat del Tractament

Gestió de les relacions contractuals, administratives, econòmiques i operatives amb proveïdors, subministradors, col·laboradors i prestadors de serveis necessaris per al desenvolupament de l'activitat de l'entitat.

Base jurídica de legitimació

- Article 6.1.b RGPD: execució de contracte.
- Article 6.1.c RGPD: compliment d'obligacions legals.

Terminis de conservació

Les dades es conservaran durant la vigència de la relació contractual. Posteriorment romandran bloquejades durant els terminis següents:

- 6 anys conforme a l'article 30 del Codi de Comerç.
- 4 anys conforme a la Llei General Tributària.
- 5 anys conforme a l'article 1964 del Codi Civil per a accions derivades de relacions contractuals.

Categories d'interessats

- Proveïdors persones físiques.
- Representants de proveïdors persones jurídiques.
- Col·laboradors externs.
- Personal de contacte d'empreses proveïdores.

Categories de dades

- Dades identificatives.
- Dades professionals.
- Dades de contacte.
- Dades econòmiques i bancàries.
- Informació contractual.

Destinataris

- Entitats financeres.
- Administracions Públiques competents.
- Assessories fiscals i comptables.
- Auditors.

Transferències internacionals

No previstes, llevat de la utilització de proveïdors tecnològics degudament regularitzats.

Mesures de seguretat

Sense perjudici de les mesures generals de conformitat amb la certificació de l'ENS indicades a l'inici del present document, d'acord amb l'article 32 del RGPD 679/2016 el responsable ha realitzat una avaluació dels riscos des del punt de vista RGPD per poder garantir els drets de les persones interessades. Sobre la base d'aquesta avaluació s'han adoptat les mesures tècniques i organitzatives necessàries, que s'han reflectit en l'informe d'anàlisi de riscos corresponent.

MESURES PER A LA PSEUDONIMITZACIÓ I EL XIFRATGE:

S'utilitzaran contrasenyes úniques i intransferibles per accedir a les dades, que no podran ser revelades a terceres persones, ni tan sols a companys de feina:

- Generació i distribució de contrasenyes

La generació de contrasenyes la realitza l'administrador del sistema, que les comunica a l'usuari que les utilitzarà.

Els sistemes que realitzin la identificació de l'usuari garantiran que la introducció de la contrasenya i la seva representació en pantalla, en el moment de l'autenticació, s'efectuen en un format no llegible per a la resta d'usuaris.

- Emmagatzematge de les contrasenyes

No està permès als usuaris anotar els identificadors i contrasenyes, ni en paper ni en suport electrònic.

- Renovació periòdica de contrasenyes

Les contrasenyes són renovades pel mateix usuari que les utilitzarà, almenys una vegada a l'any i, a més, sempre que se sospiti que la seva confidencialitat ha pogut quedar compromesa.

MESURES PER RESTAURAR LA DISPONIBILITAT I L'ACCÉS A LES DADES DESPRÉS D'UN INCIDENT:

- Còpies de seguretat

Les còpies de seguretat es realitzen diàriament en els servidors de DRIBBA DEVELOPMENT & CONSULTING SOCIEDAD LIMITADA, empresa amb la qual es manté subscrit un contracte d'Encarregat del Tractament amb els requisits contemplats a l'article 28 del RGPD. La recuperació de dades des de les còpies de seguretat s'efectuarà per l'encarregat del tractament, o amb la seva autorització i sota la seva supervisió, sempre que es produeixi una alteració, pèrdua o destrucció, total o parcial, de les dades personals, havent-se de reconstruir l'estat en què es trobaven abans de la incidència.

Quan els fitxers o tractaments afectats per la incidència estiguin parcialment automatitzats i l'existència de documentació en paper permeti la reconstrucció òptima de les dades, aquestes s'hauran d'introduir manualment i deixar constància motivada d'aquesta actuació en la descripció de la incidència.

3.- COMPTABILITAT

Finalitat del tractament

Gestió comptable, fiscal, econòmica i administrativa de l'entitat, incloent-hi l'emissió i recepció de factures, gestió de cobraments i pagaments, compliment d'obligacions tributàries i elaboració de documentació econòmico-financera.

Base jurídica de legitimació

- Article 6.1.c RGPD: compliment d'obligacions legals.
- Article 6.1.b RGPD: execució de contractes.

Terminis de conservació

Els documents comptables i fiscals es conservaran conforme a les obligacions legals següents:

- Article 30 del Codi de Comerç: 6 anys.
- Llei General Tributària (arts. 66 a 70): 4 anys.
- Llei 58/2003 General Tributària.
- Normativa mercantil i fiscal aplicable.

Finalitzats aquests terminis, les dades seran eliminades o anonimitzades, llevat que en resulti necessària la conservació per a la defensa de reclamacions judicials o administratives.

Categories d'interessats

- Clients.
- Proveïdors.
- Professionals col·laboradors.
- Representants d'entitats contractants.

Categories de dades

- Dades identificatives.
- Dades fiscals.
- Dades econòmiques i financeres.
- Dades bancàries.
- Informació relativa a operacions comercials i comptables.

Destinataris

- Agència Estatal d'Administració Tributària.
- Entitats financeres.
- Auditors.
- Administracions Públiques competents.
- Assessories fiscals i comptables.

Transferències internacionals

No previstes.

Mesures de seguretat

Sense perjudici de les mesures generals de conformitat amb la certificació de l'ENS indicades a l'inici del present document, d'acord amb l'article 32 del RGPD 679/2016 el responsable ha realitzat una avaluació dels riscos des del punt de vista RGPD per poder garantir els drets de les persones interessades. Sobre la base d'aquesta avaluació s'han adoptat les mesures tècniques i organitzatives necessàries, que s'han reflectit en l'informe d'anàlisi de riscos corresponent.

MESURES PER A LA PSEUDONIMITZACIÓ I EL XIFRATGE:

S'utilitzaran contrasenyes úniques i intransferibles per accedir a les dades, que no podran ser revelades a terceres persones, ni tan sols a companys de feina:

- Generació i distribució de contrasenyes

La generació de contrasenyes la realitza l'administrador del sistema, que les comunica a l'usuari que les utilitzarà.

Els sistemes que realitzin la identificació de l'usuari garantiran que la introducció de la contrasenya i la seva representació en pantalla, en el moment de l'autenticació, s'efectuen en un format no llegible per a la resta d'usuaris.

- Emmagatzematge de les contrasenyes

No està permès als usuaris anotar els identificadors i contrasenyes, ni en paper ni en suport electrònic.

- Renovació periòdica de contrasenyes

Les contrasenyes són renovades pel mateix usuari que les utilitzarà, almenys una vegada a l'any i, a més, sempre que se sospiti que la seva confidencialitat ha pogut quedar compromesa.

MESURES PER RESTAURAR LA DISPONIBILITAT I L'ACCÉS A LES DADES DESPRÉS D'UN INCIDENT:

- Còpies de seguretat

Les còpies de seguretat es realitzen diàriament en els servidors de DRIBBA DEVELOPMENT & CONSULTING SOCIEDAD LIMITADA, empresa amb la qual es manté subscrit un contracte d'Encarregat del Tractament amb els requisits contemplats a l'article 28 del RGPD. La recuperació de dades des de les còpies de seguretat s'efectuarà per l'encarregat del tractament, o amb la seva autorització i sota la seva supervisió, sempre que es produeixi una alteració, pèrdua o destrucció, total o parcial, de les dades personals, havent-se de reconstruir l'estat en què es trobaven abans de la incidència.

Quan els fitxers o tractaments afectats per la incidència estiguin parcialment automatitzats i l'existència de documentació en paper permeti la reconstrucció òptima de les dades, aquestes s'hauran d'introduir manualment i deixar constància motivada d'aquesta actuació en la descripció de la incidència.

4.- CONTACTES WEB I SOL·LICITUDS D'INFORMACIÓ

Finalitat del tractament

Gestió de les consultes, sol·licituds d'informació, peticions de contacte, sol·licituds comercials, incidències i qualsevol altra comunicació remesa pels usuaris a través dels formularis habilitats en el lloc web corporatiu, correu electrònic o altres canals de comunicació facilitats per SAFETROOP TECHNOLOGIES, S.L. Així mateix, aquest tractament permet mantenir comunicacions posteriors relacionades amb la sol·licitud realitzada, incloent-hi la remissió d'informació addicional sol·licitada per l'interessat i la realització d'actuacions precontractuals quan aquestes resultin necessàries.

Base jurídica de legitimació

- Article 6.1.a RGPD: consentiment de l'interessat.
- Article 6.1.b RGPD: aplicació de mesures precontractuals sol·licitades per l'interessat.

Termini de conservació

Les dades es conservaran durant el temps necessari per atendre la sol·licitud realitzada per l'interessat. Quan la consulta derivi en una relació contractual o comercial, les dades passaran a integrar-se en el tractament corresponent. En cas contrari, les dades podran conservar-se durant un termini màxim d'un any des de l'última interacció, llevat que en resulti necessari conservar-les per atendre possibles reclamacions o responsabilitats legals. Posteriorment romandran bloquejades durant el termini necessari per atendre possibles responsabilitats derivades de la relació mantinguda, de conformitat amb l'article 1964 del Codi Civil.

Categories d'interessats

- Usuaris del lloc web.
- Persones interessades en els productes o serveis de l'entitat.
- Representants d'entitats públiques o privades.
- Potencials clients.

Categories de dades

- Nom i cognoms.
- Adreça de correu electrònic.
- Telèfon de contacte.
- Entitat o organització a la qual pertany l'interessat.
- Càrrec professional.
- Contingut de la consulta o sol·licitud.
- Adreça IP i dades tècniques associades a la navegació quan procedeixi.

Destinataris

No es preveuen cessions de dades llevat d'obligació legal o quan resulti necessari per a la prestació de serveis tecnològics associats al funcionament de la pàgina web o dels sistemes de comunicació utilitzats.

Transferències internacionals

No es preveuen transferències internacionals de dades, sense perjudici de la utilització de proveïdors tecnològics que puguin implicar transferències degudament regularitzades conforme al RGPD.

ACTIVITATS COM A ENCARREGAT DEL TRACTAMENT

1.- GESTIÓ D'USUARIS AGENTS AUTORITZATS

Finalitat del tractament

Prestació de serveis tecnològics d'alerta, coordinació operativa i assistència a usuaris autoritzats pertanyents a cossos i forces de seguretat.

Base jurídica de legitimació

Prestació d'un servei i relació contractual amb el Responsable del Tractament corresponent.

Terminis de conservació

Les dades seran tractades durant la vigència del servei contractat i conforme a les instruccions documentades de l'entitat responsable del tractament. Finalitzada la prestació, les dades seran retornades, suprimides o bloquejades conforme al contracte d'encàrrec i la normativa aplicable.

Categories de dades

TIP o placa professional, identificadors d'usuari, credencials, logs d'accés, adreça IP, dades de dispositiu i geolocalització puntual associada a esdeveniments o alertes. La geolocalització únicament s'activa quan es produeix una alerta o esdeveniment de seguretat que requereix la localització de l'agent per a la seva atenció operativa.

Categories de destinataris de cessions

Administració pública, òrgan finançador.

Transferències internacionals de dades

No es realitzen transferències internacionals.

2.- GESTIÓ OPERATIVA D'ALERTES I INCIDÈNCIES

Finalitat

Tractament realitzat per compte de les entitats responsables per permetre la gestió operativa d'alertes de seguretat, incidències, esdeveniments i comunicacions associades a l'ús de la plataforma tecnològica.

Base jurídica de legitimació

La determinada per l'entitat responsable del tractament corresponent, basada en relació contractual per prestació de serveis.

Terminis de conservació

Durant el temps necessari per a la prestació del servei i conforme a les instruccions documentades del responsable del tractament. Els registres vinculats a incidents de seguretat podran conservar-se durant els terminis necessaris per garantir la investigació, traçabilitat i defensa jurídica de les actuacions realitzades.

Categories d'interessats

- Agents autoritzats.
- Usuaris operatius autoritzats per l'entitat responsable.

Categories de dades

- Identificadors professionals.
- Registres d'activitat.
- Geolocalització puntual associada a esdeveniments.
- Informació relativa a alertes.
- Marques temporals.
- Adreces IP.

Categories de destinataris de cessions

Administració pública, òrgan finançador.

Transferències internacionals de dades

No es realitzen transferències internacionals.

Mesures de seguretat

Sense perjudici de les mesures generals de conformitat amb la certificació de l'ENS indicades a l'inici del present document, d'acord amb l'article 32 del RGPD 679/2016 el responsable ha realitzat una avaluació dels riscos des del punt de vista RGPD per poder garantir els drets de les persones interessades. Sobre la base d'aquesta avaluació s'han adoptat les mesures tècniques i organitzatives necessàries, que s'han reflectit en l'informe d'anàlisi de riscos corresponent.

MESURES PER A LA PSEUDONIMITZACIÓ I EL XIFRATGE:

S'utilitzaran contrasenyes úniques i intransferibles per accedir a les dades, que no podran ser revelades a terceres persones, ni tan sols a companys de feina:

- Generació i distribució de contrasenyes

La generació de contrasenyes la realitza l'administrador del sistema, que les comunica a l'usuari que les utilitzarà.

Els sistemes que realitzin la identificació de l'usuari garantiran que la introducció de la contrasenya i la seva representació en pantalla, en el moment de l'autenticació, s'efectuen en un format no llegible per a la resta d'usuaris.

- Emmagatzematge de les contrasenyes

No està permès als usuaris anotar els identificadors i contrasenyes, ni en paper ni en suport electrònic.

- Renovació periòdica de contrasenyes

Les contrasenyes són renovades pel mateix usuari que les utilitzarà, almenys una vegada a l'any i, a més, sempre que se sospiti que la seva confidencialitat ha pogut quedar compromesa.

MESURES PER RESTAURAR LA DISPONIBILITAT I L'ACCÉS A LES DADES DESPRÉS D'UN INCIDENT:

- Còpies de seguretat

Les còpies de seguretat es realitzen diàriament en els servidors de DRIBBA DEVELOPMENT & CONSULTING SOCIEDAD LIMITADA, empresa amb la qual es manté subscrit un contracte d'Encarregat del Tractament amb els requisits contemplats a l'article 28 del RGPD. La recuperació de dades des de les còpies de seguretat s'efectuarà per l'encarregat del tractament, o amb la seva autorització i sota la seva supervisió, sempre que es produeixi una alteració, pèrdua o destrucció, total o parcial, de les dades personals, havent-se de reconstruir l'estat en què es trobaven abans de la incidència.

Quan els fitxers o tractaments afectats per la incidència estiguin parcialment automatitzats i l'existència de documentació en paper permeti la reconstrucció òptima de les dades, aquestes s'hauran d'introduir manualment i deixar constància motivada d'aquesta actuació en la descripció de la incidència.

Com s'ha exposat en el present document, les mesures organitzatives, operatives i tècniques de què disposa el Responsable del Tractament estan alineades amb l'Esquema Nacional de Seguretat (ENS), incloent-hi control d'accessos, autenticació, gestió de permisos, monitorització, traçabilitat, gestió d'incidents, protecció cloud, protecció d'aplicacions web, còpies de seguretat, continuïtat, control de canvis i desenvolupament segur.

La resta de mesures descrites en el present document són complementàries a la Declaració d'Aplicabilitat (SoA), polítiques, procediments i resta de documentació ENS de l'entitat.