

POLÍTICA DE SEGURETAT DEL PERSONAL PER AL TRACTAMENT DE DADES PERSONALS

1.- ÀMBIT D'APLICACIÓ

El Responsable del tractament està compromès a implantar una cultura de privadesa en l'organització per la qual cosa necessita que les persones autoritzades a tractar dades personals estiguin informades del tractament de dades i es responsabilitzin del mateix.

A tota persona autoritzada per tractar dades personals se li exigeix que llegeixi, compregui, compleixi i faci complir aquesta Política de seguretat per protegir les dades que formen part del tractament que li ha estat encomanat.

Aquesta Política de seguretat estableix les obligacions i procediments a seguir pel personal de l'organització, tant propi com a extern, que tracta dades personals en el desenvolupament de la seva activitat i es basa en el que es disposa en les normatives vigents en protecció de dades personals, el Reglament (UE) 2016/679 de 27 d'abril de 2016 (GDPR) i la Llei Orgànica (ES) 15/1999 de 13 de desembre (LOPD).

En aquest sentit, per vetllar i fer complir aquesta Política, l'organització ha designat un Responsable de seguretat que estarà a disposició de tot el personal i s'encarregarà de coordinar, controlar, desenvolupar i verificar el compliment de les citades normatives.

2.- CONCEPTES BÀSICS

Per proporcionar una millor comprensió de la protecció de dades, definim els principals conceptes bàsics:

Estructura del tractament:

- **Dades personals:** Informació relativa a una persona física de la qual pugui determinar-se la seva identitat.
- **Tractament:** Qualsevol operació realitzada sobre dades personals: obtenció, accés, intervenció, transmissió, conservació i supressió.
- **Interessat:** Persona física sotmesa al tractament de les seves dades personals.
- **Fitxer:** Conjunt estructurat de dades personals susceptibles de tractament per a un fi determinat.
- **Responsable del tractament:** Organització que determina les finalitats i els mitjans del tractament.
- **Personal autoritzat:** Persona autoritzada pel Responsable per realitzar un tractament de dades mitjançant un compromís de confidencialitat.



Categories de dades (nivell de seguretat):

- **Identificatius (nivell Bàsic):** Dades que no corresponguin a categories Penals o Especials, per exemple: nom, adreça, email, telèfon, edat, sexe, signatura, imatge, aficions, patrimoni, dades bancàries, informació acadèmica, professional, social, comercial, financera, etc.
- **Penals (nivell Mitjà):** Dades relatives a la comissió d'infraccions administratives o penals, o els que puguin oferir una definició de característiques de personalitat, etc.
- **Especials (nivell Alt):** Dades relatives a l'origen ètnic o racial, opinions polítiques, conviccions religioses o filosòfiques, afiliació sindical, dades genètiques o biomètrics que permetin la identificació unívoca d'una persona, dades relatives a la salut o a la vida i orientació sexuals.

3.- PRINCIPIOS DE LA PROTECCIÓ DE DADES

Els principis fonamentals per realitzar un tractament de dades són:

- **Licitud:** lleialtat i transparència amb l'interessat.
- **Limitació de les finalitats:** tractats per a finalitats determinades.
- **Minimització de les dades:** solament s'han d'obtenir les dades necessàries per aconseguir les finalitats.
- **Exactitud:** actualitzats.
- **Limitació del termini de conservació:** guardats durant no més temps del necessari per aconseguir les finalitats.
- **Integritat i confidencialitat:** aplicació de mesures de seguretat per a la protecció de les dades en totes les fases del tractament.
- **Responsabilitat proactiva:** s'ha de poder demostrar el compliment.

Consentiment per realitzar un tractament de dades

- Per tractar dades haurem d'obtenir el consentiment explícit de l'interessat i guardar el document probatori que ho acrediti.
- Quan obtinguem les dades de tercers, haurem d'assegurar-nos que la comunicació és lícita i guardar el document probatori que ho acrediti.
- No és necessari obtenir el consentiment de l'interessat quan el tractament es base en una obligació legal (per exemple, emetre una factura).

Informació del tractament a l'interessat

Haurem de facilitar la següent informació a l'interessat:

- La identitat i les dades de contacte del Responsable del tractament
- Les finalitats del tractament.
- La base jurídica del tractament.
- El termini de conservació o els criteris que ho determinin.

- Els drets que assisteixen a l'interessat.
- I si existeixen:
 - Els destinataris o categories de destinataris de les dades.
 - La transmissió de dades a països o organitzacions establertes fora de la UE.

Responsabilitat del tractament

El tractament de dades es podrà realitzar per organitzacions externes, sempre que existeixi una autorització expressa del Responsable i s'hagi subscrit un contracte per realitzar aquest tractament conforme a la legislació vigent. Per conèixer quines empreses o tercers estan autoritzats a la cessió de dades, han de dirigir-se al Responsable de seguretat.

Les organitzacions externes poden ser:

- **Encarregats del tractament:** Organització que tracta dades personals per compte del Responsable.
- **Destinataris de dades:** Organització diferent de l'Encarregat, que rep una comunicació de dades del Responsable

Mesures de seguretat

L'organització ha implementat mesures tècniques i organitzatives per garantir un nivell de seguretat adequat als riscos que pugui tenir el tractament com a conseqüència de la destrucció accidental o il·lícita de dades, la pèrdua, alteració o comunicació no autoritzada i l'accés a les dades quan són transmeses, conservades o objecte d'algun altre tipus de tractament.

El personal haurà de vetllar per la seguretat de les dades tractades per l'organització, i comunicarà al Responsable qualsevol operació de tractament que pugui suposar un risc que afecti la protecció de dades o els interessos i llibertats dels interessats.

Qualsevol disseny d'una nova operació de tractament o actualització d'una operació existent haurà de garantir abans de la seva implantació, la protecció de dades personals i l'exercici dels drets dels interessats en totes les fases del tractament: obtenció, accés, intervenció, transmissió, conservació i supressió.

4 - FUNCIONS I OBLIGACIONS DEL PERSONAL

El personal haurà d'actuar a tot moment d'acord a les instruccions detallades en l'acord de confidencialitat subscrit amb l'organització i les establertes en aquesta Política de seguretat. Amb aquesta finalitat s'estableixen les següents mesures de protecció de dades que el personal s'obliga a complir expressament:



Organització de la informació

S'hauran de classificar les dades de manera que es puguin exercir els drets dels interessats: accés, rectificació i supressió de les dades i limitació o oposició al tractament.

Conservació de les dades

S'hauran de conservar les dades en el mobiliari i departament destinats a tal fi. Per a tractaments automatitzats es guardaran els arxius en els suports, carpetes o directori de xarxa indicats pel Responsable de seguretat.

No està permès conservar dades en l'escriptori físic o digital. Solament es permet el seu tractament temporal en aquest escriptori per realitzar les operacions que ho precisin havent de ser conservades en el lloc apropiat al final de la jornada laboral.

Accés a la informació

S'hauran d'aplicar els mecanismes d'accés restringit a la informació que hagi implementat l'organització, salvaguardant les claus d'accés de tota divulgació o comunicació a altres persones.

Cada persona només està autoritzada a accedir als recursos que siguin necessaris per al desenvolupament i compliment de les seves funcions.

Es restringirà l'accés als equips informàtics mitjançant procediments de puguin identificar i autenticar la persona que accedeix als mateixos. Els noms d'usuari i contrasenya tindran la consideració de dades personals intransferibles.

Processament de dades

Els suports documentals i informàtics hauran d'estar disposats de tal forma que no siguin accessibles a persones no autoritzades

Si una persona abandona el seu lloc de treball temporalment, haurà d'ocultar els documents i bloquejar l'ordinador, de manera que s'impedeixi la visualització de la informació amb la qual estava treballant.

Quan s'utilitzin impressores o fotocopiadores, després de la impressió de treballs amb informació de caràcter personal, s'ha de recollir de manera immediata, o imprimir de forma bloquejada, assegurant-se de no deixar documents impresos en la safata de sortida.

Transport de suports

El transport de suports que continguin dades personals haurà de realitzar-se únicament per personal autoritzat o empreses externes contractades per a tal fi pel Responsable del tractament.

Eliminació de documents

Qualsevol document físic o suport digital que vulgui ser eliminat i que inclogui dades personals, ha de ser destruït amb la destructora o retirat per una empresa homologada de destrucció de documents.

Còpia de seguretat i recuperació de dades

El personal haurà d'emmagatzemar tota la informació tractada en el directori de xarxa corresponent indicat pel Responsable de seguretat, la qual cosa permetrà que a aquesta informació se li apliquin les mesures de seguretat existents i que se sotmetin els procediments de còpies de seguretat aplicats per l'organització.

Protecció de dades

S'hauran d'aplicar les mesures de protecció de dades establertes per l'organització relatius a la seguretat del tractament, com poden ser la pseudonimització o xifrat de dades o advertiments d'intrusió com a antivirus, antispam, etc.

Gestió d'incidències

Es considera una incidència a qualsevol violació de la seguretat que ocasioni la destrucció accidental o il·lícita, pèrdua, alteració, o l'accés o comunicació no autoritzats de dades personals.

El personal té l'obligació de notificar sense demora injustificada al Responsable de seguretat qualsevol incidència de què tingui coneixement perquè en prengui coneixement i l'aplicació de mesures correctives per remeiar i mitigar els efectes que hagués pogut ocasionar. Les incidències hauran de documentar-se per la persona que la notifica, amb una descripció detallada de la mateixa i la data i hora en què s'ha produït o s'ha tingut coneixement d'ella.

El coneixement i no notificació d'una incidència per part del personal es considerarà una falta contra la seguretat de les dades i podrà suposar l'inici d'accions legals, així com la reclamació de les indemnitzacions, sancions i danys o perjudicis que el Responsable es vegi obligat a atendre com a conseqüència d'aquest incompliment.