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 privacitat a l'organització pel que 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, comprengui, 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 extern, que tracta dades personals en el desenvolupament de la seva activitat i es basa en el que disposen les normatives vigents en protecció de dades personals, el Reglament (UE) 2016/679 de 27 d'abril (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 esmentades 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 per la qual es pugui determinar 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 els fins 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):

- **Identificatives (nivell Bàsic):** Dades que no corresponguin a categories Penals o especials, per exemple: nom, adreça, e-mail, 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 la vida i orientació sexuals.

3.- PRINCIPIS DE LA PROTECCIÓ DE DADES

Els principis fonamentals per realitzar un tractament de dades són:

- **Licitud**: lleialtat i transparència amb l'interessat.
- **Limitació dels fins**: tractats per a fins determinats.
- **Minimització de les dades**: només s'han d'obtenir les dades necessàries per assolir els fins.
- **Exactitud**: actualitzats.
- **Limitació del termini de conservació**: guardats durant no més temps del necessari per aconseguir els fins.
- **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 que la comunicació és lícita i guardar el document probatori que ho acrediti.
- No cal obtenir el consentiment de l'interessat quan el tractament es basi en una obligació legal (per exemple, emetre una factura).

Informació del tractament a l'interessat

Haurem facilitar la següent informació a l'interessat:

- La identitat i les dades de contacte del responsable del tractament
- Els fins 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 existeix:
  - 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 hi hagi una autorització expressa del Responsable i s'hagi subscrit un contracte per realitzar el tractament d'acord amb la legislació vigent. Per conèixer quines empreses o tercers estan autoritzats a la cessió de dades, s'han d'adreçar 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 transmesos, conservats o objecte d'algun altre tipus de tractament.

El personal ha de vetllar per la seguretat de les dades tractades per l'organització i ha de comunicar 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 ha 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 en tot moment d'acord les instruccions detallades en l'acord de confidencialitat subscrit amb l'organització i les establertes en aquesta Política de seguretat. Per a això s'estableixen les següents mesures de protecció de dades que el personal s'obliga a complir expressament:

Organització de la informació

S'hauran classificar les dades de manera que es puguin exercir els drets de les persones interessades: 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 aquest 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 a l'escriptori físic o digital. Només es permet el seu tractament temporal en dit escriptori per a realitzar les operacions que ho necessitin han de ser conservats 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 han d'estar disposats de manera que no siguin accessibles a persones no autoritzades.

Si una persona abandona el seu lloc de treball temporalment, haurà 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 no deixar documents impresos a la safata de sortida.

Transport de suports

El transport de suports que continguin dades personals s'ha de fer 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 retirats per una empresa homologada de destrucció de documents.

Còpia de seguretat i recuperació de dades

El personal ha de 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 establerts per l'organització relatius a la seguretat del tractament com poden ser la seudonimització o xifrat de dades o advertències d'intrusió com 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, qualsevol incidència que tingui coneixement al responsable de seguretat per al seu coneixement i aplicació de mesures correctives per posar remei i mitigar els efectes que hagués pogut ocasionar. Les incidències s'han de documentar 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 obligada a atendre com a conseqüència de l'incompliment.