POLÍTICA DE SEGURETAT del personal

POLÍTICA DE SEGURETAT DEL PERSONAL PER AL TRACTAMENT DE DADES PERSONALS

1.- ÀMBIT D'APLICACIÓ

El Responsable del Tractament es compromet a implantar una cultura de privacitat a l'organització, per la qual cosa necessita que les persones autoritzades a tractar dades personals estiguin informades del tractament de dades i se'n responsabilitzin.

S'exigeix a qualsevol persona autoritzada per a tractar dades personals que llegeixi, comprengui, compleixi i faci complir aquesta Política de seguretat per a protegir les dades que formen part del tractament que se li ha encomanat.

Aquesta Política de seguretat estableix les obligacions i procediments que ha de seguir el 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 estableix el Reglament (UE) 2016/679, de 27 d'abril de 2016 (GDPR), i la Llei Orgànica 3/2018, de 5 de desembre (LOPDGDD).

En aquest sentit, per vetllar pel compliment d'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 a 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 pugui determinar-se'n la 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 una finalitat determinada.
- **Responsable del tractament**: Organització que determina les finalitats i els mitjans del tractament.
- **Personal autoritzat**: Persona autoritzada pel Responsable per a realitzar un tractament de dades mitjançant un compromís de confidencialitat.

Categories de dades:

- **Bàsiques**: Dades que no corresponguin a categories Penals o Especials, per exemple: nom, adreça, e-mail, número de telèfon, edat, sexe, firma, imatge, aficions, patrimoni, dades bancàries, informació acadèmica, professional, social, financera, etc.
- **Penals**: Dades relatives a la comissió d'infraccions administratives o penals, o dades que puguin oferir una definició de característiques de personalitat, etc.
- **Especials**: Dades relatives a l'origen ètnic o racial, opinions polítiques, conviccions religioses o filosòfiques, afiliació sindical, dades genètiques o biomètriques que permetin la identificació unívoca d'una persona, dades relatives a la salut o a la vida i orientació sexuals.

3.- PRINCIPIS DE LA PROTECCIÓ DE DADES

Els principis fonamentals per a efectuar un tractament de dades són:

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

Consentiment per efectuar un tractament de dades

- Per a tractar dades cal obtenir el consentiment explícit de l'interessat i guardar el document probatori que ho acrediti.
- Si s'obtenen les dades de tercers, cal assegurar-se que la comunicació sigui lícita i guardar el document probatori que ho acrediti.
- No cal obtenir el consentiment de l'interessat si el tractament es basa en una obligació legal (per exemple, per emetre una factura).

Informació del tractament a l'interessat

Caldrà facilitar la següent informació:

- La identitat i les dades de contacte del Responsable del tractament
- Les finalitats del tractament.
- La base jurídica del tractament.
- El termini de conservació de les dades o els criteris que ho determinin.
- Els drets que té l'interessat.
- I en cas que n'hi hagi:
    - Els destinataris o categories de destinataris de les dades.

- La transmissió de dades a països o organitzacions establerts fora de l'UE.

Responsabilitat del tractament

El tractament de dades es pot efectuar per part d'organitzacions externes, sempre que hi hagi una autorització expressa del Responsable i s'hagi subscrit un contracte per a efectuar aquest tractament de conformitat amb la legislació vigent. Per saber quines empreses o tercers estan autoritzats a la cessió de dades, cal que es dirigeixin 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 personals del Responsable.

Mesures de seguretat

L'organització ha implementat mesures tècniques i organitzatives per garantir un nivell de seguretat adequat als riscos que pugui comportar 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 ha de vetllar per la seguretat de les dades que es tracten a 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 d'implantar-se, 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 ha d'actuar en tot moment d'acord amb les instruccions que es detallen a l'acord de confidencialitat subscrit amb l'organització i les que estableix aquesta Política de Seguretat. Per aquest motiu, s'estableixen, a continuació, les mesures de protecció de dades que el personal es compromet a complir expressament:

Organització de la informació

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

Conservació de les dades

S'han de conservar les dades al mobiliari i departament destinats a aquesta finalitat. Per a tractaments automatitzats, cal guardar els arxius als suports, carpetes o directori de xarxa que indiqui el Responsable de seguretat.

No és permès de conservar dades a l'escriptori físic o digital. Només se'n permet el tractament temporal a l'escriptori per a efectuar les operacions que ho requereixin, sempre que es conservin al lloc adequat en finalitzar la jornada laboral.

Accés a la informació

S'han d'aplicar els mecanismes d'accés restringit a la informació que hagi implementat l'organització i protegir les claus d'accés de qualsevol 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.

Cal restringir l'accés als equips informàtics mitjançant procediments que puguin identificar i autenticar la persona que hi accedeixi. Els noms d'usuari i les contrasenyes tenen consideració de dades personals intransferibles.

Processament de dades

Els suports documentals i informàtics han d'estar disposats de tal manera que no siguin accessibles a persones no autoritzades.

Si una persona abandona el seu lloc de treball temporalment, ha d'ocultar els documents i bloquejar l'ordinador, de manera que no sigui possible la visualització de la informació amb què està treballant.

Quan s'utilitzin impressores o fotocopiadores, després de la impressió de treballs amb informació de caràcter personal, cal recollir-los immediatament, o imprimir de forma bloquejada, i assegurar-se de no deixar documents impresos a la safata de sortida.

Transport de suports

El transport de suports que contingui dades personals només el pot dur a terme el personal autoritzat o empreses externes contractades per a aquesta finalitat pel Responsable del tractament.

Eliminació de documents

Qualsevol document físic o suport digital que s'hagi d'eliminar i que inclogui dades personals s'ha de destruir amb la destructora o ha de ser retirat per una empresa homologada de destrucció de documents.

Còpia de seguretat i recuperació de dades

El personal ha d'emmagatzemar tota la informació tractada al directori de xarxa corresponent indicat pel Responsable de Seguretat, la qual cosa permetrà que s'hi apliquin les mesures de seguretat

existents i que es duguin a terme els procediments de còpies de seguretat aplicats per l'organització.

Protecció de dades

S'han d'aplicar les mesures de protecció de dades que estableix l'organització en relació amb la seguretat del tractament, com ara la pseudonimització o xifrat de dades o advertències d'intrusió com antivirus, *antispam*, etc.

Gestió d'incidències

Es considera una incidència qualsevol violació de la seguretat que tingui com a conseqüència 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 descobreixi al Responsable de seguretat per a tenir-ne coneixement i per a l'aplicació de mesures correctores per a posar remei i mitigar els efectes que pugui haver ocasionat. La persona que notifica la incidència ha de documentar-la amb una descripció detallada i la data i hora en què s'ha produït o se n'ha tingut constància.

Ésser conscient d'una incidència per part del personal i no notificar-la es considera una falta contra la seguretat de les dades i pot suposar l'inici d'accions legals, així com la reclamació d'indemnitzacions, sancions i danys o perjudicis que el Responsable es vegi obligat a atendre com a conseqüència d'aquest incompliment.