Protecció de dades. Per on començo?

El Prat de Llobregat, 8 de Febrer de 2020

Montse Agudo

EMAS ES-CAT-275

ISO 9001 10121

Applus ISO 14001 10168

@ diba
@suport_org

Que treballarem avui?

1. Principals conceptes i obligacions de la protecció de dades
2. Exemple Registre d'activitats de tractament
3. Models dels principals avisos legals
4. Eines i recursos (Facilita i Gestiona)

Què és la Protecció de Dades?

Què és la Protecció de Dades?

- **Concepte**:

És el dret que te tota persona a exercir un control efectiu sobre les dades relatives a la seva pròpia persona.

- **Persones obligades**:

Qualsevol empresa, autònom, fundació, associació, i administració pública que tracti dades de persones físiques

- **Dades que són objecte de protecció**:

Qualsevol tipus d'informació: Informació alfabètica, numèrica (telèfon, IP, etc.), imatges (fotografies, imatges de càmeres de vídeo vigilància, etc.), informació acústica (gravacions de veu), adreça de correu electrònic, etc., que puguin fer identificables a persones físiques

Què és la Protecció de Dades?

- **Tractament de dades:**

Operacions i procediments (de caràcter automatitzat o no) que permetin la recollida, gravació, conservació, elaboració, modificació, consulta, utilització, modificació, bloqueig i supressió, així com les cessions de dades que resultin de comunicacions, consultes interconnexions i transferències.

Normativa aplicable

Canvi de paragdima

REACTIU
LOPD

PROACTIU
RGPD
DIMENSIÓ PREVENTIVA

Article 1 RGPD

OBJECTE DEL RGPD

1.Establir unes normes relatives a:

- ✓ La protecció de les persones físiques en allò que respecta al tractament de dades personals
- ✓ La lliure circulació de les dades

2. Protegir els drets fonamentals de les persones físiques en quant a les seves dades personals

Principis: art. 5 RGPD

- Licitud, lleialtat i transparència
- Limitació de la finalitat
- Minimització de les dades
- Exactitud
- Limitació del termini de conservació
- Integritat i confidencialitat

Principals obligacions i tasques

- **Obligacions i tasques a fer**:
  - ✓ Identificació de les dades que tenim i el seu nivell de sensibilitat
  - ✓ Establir base de licitud
  - ✓ Deure d'informació
  - ✓ Obtenció del consentiment per a la cessió de dades
  - ✓ Registres de tractament d'activitat
  - ✓ Respecte i compliment dels drets dels titulars de les dades
  - ✓ Identificació dels riscos
  - ✓ Manual de Seguretat
  - ✓ Document d'avaluació d'impacte*

- Reglament Europeu 2016/679 de protecció de dades personals

Bases de Licitud

- Consentiment exprés
- Relació contractual
- Interès legítim
- Interès públic

Nou règim pel consentiment

El consentiment ha de donar-se mitjançant ACTE AFIRMATIU CLAR que reflecteixi una manifestació de VOLUNTAT LLIURE, ESPECÍFICA, INFORMADA I INEQUÍVOCA

- IMPORTANT: Si el consentiment sobre base escrita. S'ha de diferenciar clarament dels altres assumptes. Llenguatge clar i de fàcil accés
- Les caselles pre-marcades o la inacció no han de constituir consentiment

EL CONSENTIMENT HA DE FACILITAR-SE PER A TOTES LES ACTIVITATS DE TRACTAMENT REALITZADES AMB LA MATEIXA FINALITAT.

Si el tractament té diverses finalitats, ha de donar-se el consentiment per totes elles.

El responsable del tractament ha de ser capaç de demostrar que l'interessat ho ha prestat per a aquesta fi concreta. CÀRREGA DE LA PROVA

DRET A REVOCAR CONSENTIMENT A QUALSEVOL MOMENT

Avisos legals

Els avisos legals han de contenir:

- ✓ Informació identificadora del responsable de les dades
- ✓ Tractament que en farà
- ✓ Finalitat del tractament de les dades
- ✓ Termini de conservació
- ✓ Cessió de dades
- ✓ Drets que pot exercir el titular
- ✓ Possibilitat de reclamació davant l'Autoritat de control
- ✓ Identificació del DPD, si s'escau

Registres d’activitat de tractament

Els responsables i encarregats del tractament hauran de dur un registre de tractament d’activitats efectuades sota la seva responsabilitat.

*Model

Anàlisi de Riscos

PODEM ESTABLIR DUES TIPOLOGIES D'ANÀLISI SEGONS LA COMPLEXITAT DELS RESPONSABLES:

1.Grans organitzacions: Com a regla general, en aquests casos l'anàlisi haurà de dur-se a terme utilitzant alguna de les metodologies d'anàlisis de risc existents.

1.Organitzacions petites amb tractaments de poca complexitat: l'anàlisi serà resultat d'una reflexió documentada sobre les implicacions dels tractaments en els drets i llibertats dels interessats. S'analitzaran qüestions com les següents i quantes més respostes afirmatives, major serà el risc que podria derivar-se d'aquest tractament.

Document d'avaluació d'impacte

El document d'avaluació d'impacte és una eina que permet avaluar de manera anticipada quins són els riscos potencials als quals s'està exposat en funció del tractament que es fa de les dades personals dins de l'entitat.

- **Facilita**
- **Gestiona**

Els nous drets dels afectats

- Informació + consentiment
- ELS ARCO: accés, rectificació, cancel·lació, oposició
- Novetats:
  - ✓ DRET A L'OBLIT (SUPRESSIÓ)
  - ✓ DRET A LA PORTABILITAT
  - ✓ DRET A LA LIMITACIÓ DE TRACTAMENT

Mesures de Seguretat

- EL nou RGPD recull entre els seus principis rectors, llistats al seu article 5, el principi d'integritat i confidencialitat (en la seva lletra f), que estableix

"Tractats de tal manera que es garanteixi una seguretat adequada de les dades personals, inclosa la protecció contra el tractament no autoritzat o il·lícit i contra la seva pèrdua, destrucció o dany accidental, mitjançant l'aplicació de mesures tècniques o organitzatives apropiades"

- No obstant això, NO trobem en la norma un CATÀLEG de mesures per garantir el compliment d'aquest principi. Com podem llavors aplicar les mesures de seguretat adequades?

CONCLUSIÓ: LES QUE VULGUIS EN FUNCIÓ DELS RISCOS QUE TINGUIS…

Principals Mesures de Seguretat

- Informació sobre el tractament a totes les persones de l'entitat.
- Deure de secret i confidencialitat.
- Accés restringit a les dades personals (permisos, contrasenyes, etc.)
- Contrasenyes: alfanumèriques de 8 dígits mínim. Renovació periòdica.
- Guardar les dades personals als llocs habilitats (programari, carpetes, etc.)
- Bloqueig de pantalla quan no s'està treballant i apagar l'equip al finalitzar.
- Ordinadors personals: sessions diferenciades.
- Suports electrònics (memòria externa, llapis...) en lloc segur i restringit.
- Esborrat efectiu de les dades en suport electrònic.
- Enviament xifrat de les categories especials de dades.
- Actualització dels sistemes informàtics.

Principals Mesures de Seguretat

- Antivirus i tallafocs actualitzat.
- Còpies de seguretat periòdiques. Emmagatzematge en un lloc diferent al lloc habitual de treball o en una caixa ignífuga.
- Documentació en paper en lloc segur i accés restringit.
- Custodia de les claus d'accés a arxivadors o dependències (armaris, despatx..)
- Tancament de la ubicació amb clau al final de la jornada laboral o en cas d'absència a fi d'evitar accessos no autoritzats.
- No deixar documents amb dades a la fotocopiadora, impressora, taula quan no hi som...
- Trasllat de documentació en paper amb seguretat.
- Destructora de paper.
- Revisió habitual de les mesures establertes en relació a la protecció de dades.
- Comunicació de les violacions de seguretat a la AEPD en 72h màxim.

Què és això del DPD?

Càrrec:

- Encarregat d'assessorar i supervisar el responsable o encarregat del tractament.
- Interlocució amb l'AEPD i els afectats.
- Coneixements avançats en la matèria.
- Capacitats per executar el RGPD i suficientment qualificat i/o certificat.

Principals funcions del DPD:

- Realitza auditories
- Realitza avaluacions d'impacte
- Aplica i implementa polítiques de protecció de dades
- Assigna responsabilitats
- Forma al personal i el consciència

Obligació a tenir DPD (art.37 RGPD)

- Empreses de més de 250 treballadors
- Empreses que treballin en grup d'empreses
- Tracten dades de categories especials (orientació sexual, salut, creences, opinions polítiques, afiliació sindical, origen racial o étnic, dades biomètriques o genètiques).
- Tracten dades d'infraccions penals o condemnes. Amb un volum important.
- La seva activitat principal requereix tractament de dades personals a gran escala. Realitzen un seguiment habitual i continu de dades personals, creant perfils.
- Són organisme o autoritat pública

Dret d'imatge

- La llei intenta evitar que la imatge de persones sense projecció pública sigui captada de manera que es pugui reconèixer, reproduïda o publicada sense el seu consentiment , facultat que només l'interessat pot exercir

- Sempre s'ha de demanar autorització per captar la imatge, reproduir-la i publicar-la. Són tres actes diferents, per tant, cal demanar autorització per les tres coses.

- L'autorització ha de ser expressa i ha de constar per un mitjà demostrable. En cas de no disposar d'autorització, no es poden captar ni difondre imatges dels menors o bé no han de ser recognoscible.

Sancions per incompliment

- Fins a 20 milions d'euros o el 4% del volum de negoci de l'entitat

Fundesplai
Suport Tercer Sector

Moltes gràcies!!

Federació Catalana de l'Esplai | Fundesplai

www.suport.org

@ diba

@suport_org