connecTerrassa

RGPD - Protecció de dades

Terrassa, 16 de Maig de 2018

àbac ASSESSORS

connecTerrassa

Què són les dades personals?

Les DADES PERSONALS són tota la informació sobre una persona física (interessat) identificada o identificable.

Són dades personals: un nom, un número d'identificació (DNI, NIE, passaport, etc.), les dades de localització (adreça, adreça electrònica, adreça IP, etc.), un identificador en línia, els elements propis d'identitat física (fotografies i característiques físiques), fisiològica, genètica, psíquica, econòmica, cultural o social, etc.

Les dades de les **persones jurídiques** (empreses, associacions, fundacions, etc.) **NO queden incloses** dins de la definició de "dades personals" i per tant, no tenen el mateix tractament.

Si a les bases de dades es disposa de dades de les persones físiques (p.e. treballadors) d'una persona jurídica, s'hauran de separar les dades que són pròpiament de la persona jurídica i les que ho són de les persones físiques que hi estan vinculades, i aplicar els mecanismes de control i seguretat per separat.

Quins són els drets dels ciutadans?

Els antics drets ARCO

- Accés
- Rectificació
- Cancel·lació
- Oposició

I els nous drets RPGD

- Transparència
- Oblit
- Limitació del tractament
- Portabilitat de les dades

Què és el nou RGPD?

RGPD = Reglament General de Protecció de Dades

És una normativa EUROPEA que preval per sobre de la normativa estatal espanyola, i que és i serà de COMPLIMENT OBLIGATORI

Diferències entre la antiga LOPD i el nou RGPD:

1) **Abast de la norma**: Espanya vs. Europa
2) Obligatorietat del **consentiment EXPRÉS**
3) Nou **dret d'informació** a l'interessat
4) Principi de **responsabilitat PROACTIVA**
   a. Anàlisi de riscos
   b. Protocols de seguretat (seguretat informàtica)
   c. La figura del delegat de protecció de dades (DPO)
   d. Auditories periòdiques i organismes de certificació
   e. Règim sancionador: en casos extrems, fins al 4% de la xifra de negoci o 20 milions d'€

Consentiment EXPRÉS

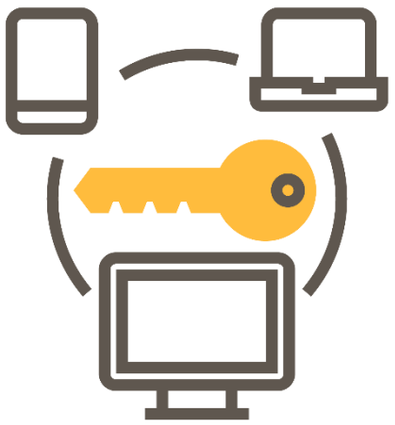
- ✓ El consentiment que presta l'interessat per a la gestió de les seves dades haurà de ser inequívoc, clarament favorable i donat de forma expressa. Per tant, contràriament al que actualment permet la normativa espanyola, queda exclòs el consentiment tàcit.

- ✓ El consentiment està basat en una declaració de l'interessat o una acció positiva. El silenci o les caselles pre-marcades, no seran consentiments vàlids.

- ✓ Els consentiments expressos anteriors a la data del nou RGPD i de la seva entrada en vigor continuaran sent vàlids si compleixen aquests requisits.

Principi de responsabilitat proactiva

SEGURETAT INFORMÀTICA



Amb el RGPD s'amplia el contingut dels protocols de seguretat, incorporant mencions obligatòries quant als procediments i al reforç de les mesures de seguretat informàtica, sobretot en els casos dels tractaments automatitzats o en els accessos remots a les dades, ja sigui per connexions remotes o a través de dispositius mòbils (smartphones, tablets, portàtils, etc.).

Les mesures de seguretat a implementar per cada empresa/activitat hauran de determinar-se amb la finalitat de garantir un nivell de seguretat adequat en funció del risc existent (prèvia anàlisi del risc) i tenint en compte:

- La naturalesa, àmbit, context i finalitat de les dades
- El risc en el tractament en relació amb els drets i llibertats de les persones
- L'estat de la tècnica i cost d'aplicació de les mesures de seguretat

Implementació del nou RGPD?

- Registrar els fitxers:
  Ara mateix, amb el RGPD, no hi ha l'"obligació" del registre dels fitxers "de forma estricta" com estava configurada fins ara, si bé es crea l'obligació de registrar les activitats de tractament.
- Tenir confeccionat i aprovat el seu document de seguretat
- Aplicar els protocols de control i gestió en la protecció de dades
  - Gestió de tots els consentiments expressos
  - Gestió de tots els contractes pertinents amb els tercers que tinguin accés a dades durant el procés del tractament (gestors i assessors, informàtics, empreses de neteja, destrucció de documents, gestió de servidors i còpies de seguretat, etc.)
- Realitzar els controls i les auditories de compliment.

Registre Activitats de Tractament

El nou Registre d'Activitats del Tractament CONTINDRÀ:

- Identificació i dades de contacte del responsable, representant i DPO
- La finalitat del tractament de les dades
- Definició de categories d'interessats i de dades
- Període de conservació i terminis previstos per la supressió de les dades
- Descripció general de les mesures de seguretat.

Règim sancionador

No hi ha categories de sancions. S'estudiarà cada cas concret valorant:

- La naturalesa, la gravetat i la duració de la infracció
- La intencionalitat (*dolo*) o la negligència
- Les mesures de control posades pel responsable per reduir els danys causats
- El grau de responsabilitat del responsable
- L'existència d'antecedents (infraccions anteriors)
- El grau de cooperació amb les autoritats de control per posar remei a la infracció
- La categoria de les dades personals afectades
- La forma en què l'autoritat de control va tenir coneixement de la infracció. (*Serà diferent que la infracció la notifiqui el mateix responsable, que si la notifica el perjudicat.*)
- L'adhesió a codis de conducta o mecanismes de certificació aprovats (***per a un futur***)
- Existència d'agreujants o atenuants de la responsabilitat

Les sancions poden arribar fins als 20 milions d'euros o el 4% de la xifra de negoci.

Com afecta el meu negoci?

Check list intern de situació inicial de riscos:

L'anàlisi de riscos depèn de:

1. L'activitat de l'empresa/negoci
2. La mida de l'empresa/negoci
3. La naturalesa de les dades
4. El tractament que es farà de les dades
5. Els sistemes de tractament i custòdia de dades (seguretat informàtica)

I obtindrem una classificació de nivell de seguretat

1. Bàsic
2. Mitjà
3. Alt

Exemples de gestió documental

Els contractes sempre per escrit i han de detallar les instruccions del responsable a l'encarregat del tractament, en relació a les mesures de seguretat. També ha de constar el règim de subcontractació i la confidencialitat.

1) Document de presa de dades de clients i proveïdors. Model Àbac i de nivell alt.

2) Clàusules en els contractes amb els treballadors. Model Àbac (inclou altres aspectes com confidencialitat, ús de les TICs, etc.)

3) Com gestionar un dia qualsevol – infografia 1 de SAGE

4) El RGPS a cop d'ull – infografia 2 de SAGE

Preguntes que ens hem fer (1):

a. S'han de protegir totes les dades? Les dades de les empreses també? Es necessita el consentiment de les empreses?
b. El nou RGPD afecta una petita empresa amb pocs treballadors que no tracta amb consumidors finals?
c. Tens ben identificats i controlats els consentiments de forma inequívoca i explícita per utilitzar-los? Guardes els consentiments? Quant de temps?
d. Amb qui he de signar contractes o protocols de seguretat i confidencialitat?
e. I amb els treballadors, què m'interessa signar? Clàusules protecció de dades, TICs i confidencialitat.

Preguntes que ens hem fer (2):

f. Si tinc una violació de la seguretat de les dades personals, què he fer?
g. Nou règim sancionador. N'he de tenir por?
h. Em puc oposar a rebre comunicacions per correu electrònic?
i. S'han de continuar registrant els fitxers davant l' *AEPD*?
j. Què son les cookies i per a què serveixen?
k. A una comunitat de propietaris o una entitat sense ànim de lucre, els afecta el RGPD?
l. Què es la política de privadesa del web?
m. Què és la LSSI-CE?
n. La política de contractació en serveis o venda *online*, afecta la protecció de dades?

I la pregunta de l'e-mail marketing

Tinc una BD de contactes que he treballat durant molts anys. A partir d'ara **ja no la puc utilitzar?**

a. Sí, si puc demostrar el consentiment explícit dels interessats.

b. Per als que NO en tinc el consentiment:

   1. Els l'he de demanar
   2. Si no l'obtinc, perquè s'hi neguen o no responen, els he d'eliminar de la BD.

Moltes gràcies per la seva atenció

Ester Hervàs
Advocada
ester@abac.cat

Amb la col·laboració i material cedit per

sage | Professional Advisor

àbac ASSESSORS

àbac ASSESSORS

Professional Advisor

Puntos de Atención al Emprendedor

Promotor de hub TERRASSA

Av. Jaume I, 95 1r
08226 Terrassa

Tel. 93 736 98 60
abac@abac.cat

@AbacAssessors
www.abac.cat