FORMA'T I TRANSFORMA
www.peretarres.org/**acciosocial**

FORMACIÓ
per a entitats
i empreses

GENERA TALENT SOCIAL

QUALITAT + EXPERTESA = TALENT²

Protecció de dades personals:
la nova normativa europea

FUNDACIÓ
PERE TARRÉS

FORMACIÓ per a entitats i empreses
GENERA TALENT SOCIAL

NOM DEL MATERIAL: Protecció de dades personals la nova normativa europea

DATA EDICIÓ: Juliol 2018

NÚMERO EDICIÓ: 1a

AUTORIA DEL MATERIAL: Carlota Palet Vendrell

Coordinació de continguts: Laura Flores

FUNDACIÓ PERE TARRÉS

1.-EL REGLAMENT EUROPEU DE PROTECCIÓ DE DADES

El Reglament General de Protecció de Dades (RGPD) comença a **aplicar-se el 25 de maig de 2018.**

El Reglament s'aplicarà com fins ara a responsables o encarregats de tractament de dades establertes en la Unió Europea, i s'amplia a responsables i encarregats no establerts en la UE sempre que realitzin tractaments derivats d'una oferta de béns o serveis destinats a ciutadans de la Unió o com a conseqüència d'un monitoratge i seguiment del seu comportament.

Perquè aquesta ampliació de l'àmbit d'aplicació pugui fer-se efectiva, aquestes organitzacions hauran de nomenar un representant en la Unió Europea, que actuarà com a punt de contacte de les Autoritats de supervisió i dels ciutadans i que, en cas necessari, podrà ser destinatari de les accions de supervisió que desenvolupin aquestes autoritats. Les dades de contacte d'aquest representant en la Unió hauran de proporcionar-se als interessats entre la informació relativa als tractaments de les seves dades personals.

Aquesta novetat suposa una garantia addicional als ciutadans europeus. En l'actualitat, per tractar dades no és necessari mantenir una presència física sobre un territori, per la qual cosa el Reglament pretén adaptar els criteris que determinen què empreses han de complir-ho a la realitat del món d'internet.

Això permet que el Reglament sigui aplicable a empreses que, fins ara, podien estar tractant dades de persones en la Unió i, no obstant això, es regien per normatives d'altres regions o països que no sempre ofereixen el mateix nivell de protecció que la normativa europea.

El RGPD és una norma directament aplicable, que no requereix de normes internes de trasposició ni tampoc, en la majoria dels casos, de normes de desenvolupament o aplicació. Per això, els responsables deuen abans de res assumir que la norma de referència és el RGPD i no les normes nacionals, com venia succeint fins ara amb la Directiva 95/46. No obstant això, la llei que substituirà a l'actual Llei Orgànica de Protecció de Dades (LOPD) sí podrà incloure algunes precisions o desenvolupaments en matèries en les quals el RGPD ho permet. El RGPD conté molts conceptes, principis i mecanismes similars als establerts per la Directiva 95/46 i per les normes nacionals que l'apliquen. Per això, les organitzacions que en l'actualitat compleixen adequadament amb la LOPD espanyola tenen una bona base de partida per evolucionar cap a una correcta aplicació del nou Reglament. No obstant això, el RGPD modifica alguns aspectes del règim actual i conté noves obligacions que han de ser analitzades i aplicades per cada organització tenint en compte les seves pròpies circumstàncies.

Dos elements de caràcter general constitueixen la major innovació del RGPD per als responsables i es projecten sobre totes les obligacions de les organitzacions:

1.1.- El principi de responsabilitat proactiva

El RGPD descriu aquest principi com la necessitat que el responsable del tractament **apliqui mesures tècniques i organitzatives apropiades a fi de garantir i poder demostrar que el tractament és conforme amb el Reglament.** En termes pràctics, aquest principi requereix que les organitzacions analitzin quines dades tracten, amb quines finalitats ho fan i quin tipus d'operacions de tractament duen a terme. A partir d'aquest coneixement han de determinar de forma explícita la forma en què aplicaran les mesures que el RGPD preveu, assegurant-se que aquestes mesures són les adequades per complir amb el mateix i que poden demostrar-ho davant els interessats i davant les autoritats de supervisió.

En síntesi, aquest principi exigeix una actitud conscient, diligent i proactiva per part de les organitzacions enfront de tots els tractaments de dades personals que duguin a terme.

1.2.- L'enfocament de risc

El RGPD assenyala que les mesures dirigides a garantir el seu compliment han de tenir en compte la naturalesa, l'àmbit, el context i les finalitats del tractament així com **el risc per als drets i llibertats de les persones.**

D'acord amb aquest enfocament, algunes de les mesures que el RGPD estableix s'aplicaran només quan existeixi un alt risc per als drets i llibertats, mentre que unes altres hauran de modular-se en funció del nivell i tipus de risc que els tractaments presentin.

L'aplicació de les mesures previstes pel RGPD ha d'adaptar-se, per tant, a les característiques de les organitzacions. El que pot ser adequat per a una organització que maneja dades de milions d'interessats en tractaments complexos que involucren informació personal sensible o volums importants de dades sobre cada afectat no és necessari per a una petita empresa que duu a terme un volum limitat de tractaments de dades no sensibles.

2.- LA LEGITIMACIÓ PER AL TRACTAMENT DE DADES

El RGPD manté el principi recollit en la Directiva 95/46 que tot tractament de dades necessita recolzar-se en una base que ho legitimi.

També recull les mateixes bases jurídiques que contenia la Directiva i que reprodueix la LOPD:

- Consentiment.
- Relació contractual.
- Interessos vitals de l'interessat o d'altres persones.
- Obligació legal per al responsable.
- Interès públic o exercici de poders públics.
- Interessos legítims prevalents del responsable o de tercers als quals es comuniquen les dades. En aquest sentit, el RGPD no implica canvis per als responsables del tractament de dades.

Així es recomana per la RGPD que hauria d'incloure's la base legal sobre la qual es desenvolupa el tractament en proporcionar informació al moment de la recollida de dades i especificar els interès legítims en què es fonamenten les operacions de tractament.

"El consentiment ha de ser "inequívoc"

El consentiment inequívoc és aquell que s'ha prestat mitjançant una manifestació de l'interessat o mitjançant una clara acció afirmativa. **A diferència del Reglament de Desenvolupament de la LOPD, no s'admeten formes de consentiment tàcit o per omissió, ja que es basen en la inacció**

Es contemplen situacions en les quals el consentiment, a més d'inequívoc, ha de ser explícit:

- Tractament de dades sensibles.
- Adopció de decisions automatitzades.
- Transferències internacionals.

El consentiment pot ser inequívoc i atorgar-se de forma implícita quan es dedueixi d'una acció de l'interessat (per exemple, quan l'interessat continua navegant per una web i accepta així el que s'utilitzin cookies para monitoritzar la seva navegació).

Els tractaments iniciats amb anterioritat a l'inici de l'aplicació del RGPD sobre la base del consentiment seguiran sent legítims sempre que aquest consentiment s'hagués prestat de la manera en què preveu el propi RGPD, és a dir, mitjançant una manifestació o acció afirmativa.

Si alguna empresa o entitat havia obtingut el consentiment per omissió haurà de dur a terme una acció per obtenir el consentiment explicito.

3.- TRANSPARÈNCIA I INFORMACIÓ ALS INTERESSATS

La informació als interessats, tant respecte a les condicions dels tractaments que els afectin com en les respostes als exercicis de drets, haurà de proporcionar-se de forma **concisa, transparent, intel·ligible i de fàcil accés, amb un llenguatge clar i senzill**.

(La LOPD només exigeix que la informació es presti de manera expressa, precís i inequívoc)

Pel que s'hauran d'evitar les fórmules especialment desmanegades i que incorporen remissions als textos legals.

Les clàusules informatives hauran d'explicar el contingut al que immediatament es refereixen de forma clara i accessible per als interessats, amb independència dels seus coneixements en la matèria.

S'estableix una llista exhaustiva de la informació que ha de proporcionar-se als interessats (més àmplia que la que actualment conté la LOPD) i que afegeix:

- Base jurídica del tractament
- Intenció de realitzar transferències internacionals
- Dades del Delegat de Protecció de Dades (si ho hi hagués)
- Elaboració de perfils

La informació als interessats haurà de facilitar-se per escrit, inclosos els mitjans electrònics quan sigui apropiat.

L'AEPD, Autoritat Catalana de Protecció de Dades i Agència Basca de Protecció de Dades han preparat una Guia sobre el dret a la informació que pot consultar-se: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf

4.- RELACIONS RESPONSABLE-ENCARREGAT

Hi ha 3 novetats que els responsables i encarregats han de prendre en consideració:

4.1.- Obligacions específiques per als encarregats

El RGDP conté obligacions expressament dirigides als encarregats:

- Els encarregats tenen obligacions pròpies que estableix el RGPD, que no se circumscriuen a l'àmbit del contracte que els uneix al responsable, i que poden ser supervisades separadament per les autoritats de protecció de dades.

Per exemple:

- **Han de mantenir un registre d'activitats de tractament.**
- **Han de determinar les mesures de seguretat aplicables als tractaments que realitzen.**
- **Han de designar a un Delegat de Protecció de Dades en els casos previstos pel RGPD.** Una de les exigències que introdueix el RGDP és la contractació d'un delegat de protecció de dades (DPO, per les seves sigles en anglès: data protection officer) en determinats suposats. La norma no precisa els casos en els quals serà necessari contractar amb el DPO a través determinar una quantitat de dades tractades, persones afectades pel tractament o l'àmbit dels mateixos, sinó que ofereix una descripció general dels supòsits en què serà obligatori.

L'article 37 del Reglament determina l'obligatorietat de la designació del DPO:

- Quan el tractament ho dugui a terme una autoritat o organisme públic.
- Quan les activitats principals del responsable o encarregat del tractament consisteixin en operacions de tractament que requereixin un seguiment regular i sistemàtic dels interessats a gran escala.
- Quan les activitats principals del responsable o l'encarregat consisteixin en el tractament a gran escala de categories especials de dades o dades personals relacionades amb condemnes i delictes.

El primer dels tres supòsits afecta a les Administracions i ens del sector públic, en els quals es plantegen menys dubtes.

Els altres dos sí empren alguns conceptes més indeterminats i que requereixen una major precisió.

"**Activitats principals"**

Quan els dos segons apartats es refereixen a les "activitats principals del responsable o l'encarregat del tractament" parlen de l'activitat primària de l'empresa, i no aquelles en les quals el tractament de dades sigui una funció auxiliar.

S'entendrà que estem davant una activitat principal quan el tractament de dades sigui l'objectiu fonamental de la mateixa (una app que maneja perfils, per exemple), o bé, quan el tractament resulti part intrínseca de l'actuació de l'empresa. En aquest segon suposat, per exemple, encaixaria el cas d'un hospital en el qual, si ben finalitat principal és la prestació de serveis sanitaris, aquests no podrien prestar-se sense operar amb les dades dels pacients. En conseqüència, l'hospital haurà de contractar un DPO.

En l'altre extrem, el processament de dades dels empleats necessari per al pagament de nòmines, per exemple, no tindrà la consideració d'activitat principal sinó d'activitat auxiliar. Així, no donarà lloc a l'obligació de contractar un delegat.

"A gran escala"

El Reglament no especifica una xifra de dades tractades o persones afectades que permet considerar que el tractament és "a gran escala".

De moment, els elements que han de tenir-se en compte per precisar si el tractament és "a gran escala" són: la quantitat de persones afectades (en nombre o en proporció), el volum de dades o el ventall de diferents conceptes de dades que es processen, la durada o permanència de l'activitat de tractament de dades i l'abast geogràfic de l'activitat del tractament.

"Seguiment regular i sistemàtic"

Per "seguiment" ha d'entendre's totes les formes possibles de seguiment i creació de perfils en Internet, fins i tot a l'efecte de publicitat basada en el comportament.

En parlar de "regular" es refereix el que es realitzi de forma continuada o que es produeix en intervals concrets durant un temps concret; recurrent o repetit en moment prefixats; o que es produeix de forma constant o periòdica.

I, finalment, per "sistemàtic", és el que es produeix d'acord amb un sistema; preestablert, organitzat o metòdic; que té lloc com a part d'un pla general de recollida de dades; o, finalment, com a part una estratègia.

El DPO no pot ser acomiadat ni rebre instruccions.

El Reglament atorga un paper molt rellevant al delegat en el si de les empreses i, a més, ho blinda per convertir-ho en una autèntica figura de control intern.

En aquest sentit, les dades de contacte del DPO han de ser públics perquè qualsevol interessat o l'organisme de supervisió pugui contactar amb ell de forma fàcil, directa i confidencial, sense que aquesta comunicació transcendeixi en l'organització.

L'empresa, a més, haurà de proveir-li dels "recurs necessaris", en sentit ampli: que tingui el temps suficient per complir les seves funcions; que rebi el suport adequat quant a recursos econòmics, infraestructures i personal; que tingui accés a altres serveis i departaments (l'arxiu de recursos humans, per exemple); i, a més, que se li doti de formació contínua per mantenir el seu "coneixement expert".

En l'exercici de les seves funcions, el DPO no podrà rebre cap instrucció (ja sigui un treballador de l'empresa o organització o no) i, a més, no podrà ser acomiadat o sancionat per l'exercici de les mateixes. El concepte "sanció" ha d'entendre's en sentit ampli: estan prohibides tant les directes com les indirectes (la dilació d'un ascens, per exemple); també la mera amenaça de la mateixa.

L'AEPD ha optat per promoure un sistema de certificació de professionals de protecció de dades com a eina útil a l'hora d'avaluar que els candidats a ocupar el lloc de DPO reuneixen les qualificacions professionals i els coneixements requerits. Les certificacions seran atorgades per entitats certificadores degudament acreditades per l'Entitat Nacional d'Acreditació, seguint criteris d'acreditació i certificació elaborats per l'AEPD en col·laboració amb els sectors afectats.

La certificació no serà un requisit indispensable per a l'accés a la professió, serà només una opció a la disposició de responsables i encarregats per facilitar la seva selecció dels professionals anomenats a ocupar el lloc de DPO. Però responsables i encarregats poden prendre en consideració altres qüestions o altres mitjans per demostrar la competència dels DPO.

4.2.- Elecció de l'encarregat de tractament

Segons el RGPD, el responsable haurà d'adoptar mesures apropiades, inclosa l'elecció d'encarregats, de manera que garanteixi i estigui en condicions de demostrar que el tractament es realitza conforme el RGPD (principi de responsabilitat activa).

Els responsables hauran de triar únicament encarregats que ofereixin garanties suficients per aplicar mesures tècniques i organitzatives apropiades, de manera que el tractament sigui conforme amb els requisits del Reglament. Aquesta previsió s'estén també als encarregats quan subcontractin operacions de tractament amb altres subencarregats.

4.3.- Contingut del contracte per encàrrec

Les relacions entre el responsable i l'encarregat han de formalitzar-se en un contracte o en un acte jurídic que vinculi a l'encarregat respecte al responsable.

Es regula de forma minuciosa el contingut mínim dels contractes per encàrrec, havent de preveure's aspectes com:

- Objecte, durada, naturalesa i la finalitat del tractaments.
- Tipus de dades personals i categories d'interessats.
- Obligació de l'encarregat de tractar les dades personals únicament seguint instruccions documentades del responsable.
- Condicions perquè el responsable pugui donar la seva autorització prèvia, específica o general, a les subcontractacions.
- Assistència al responsable, sempre que sigui possible, en l'atenció a l'exercici de drets dels interessats.

Els contractes per encàrrec conclosos amb anterioritat a l'aplicació del RGPD al maig de 2018 han de modificar-se i adaptar-se per respectar aquest contingut, sense que siguin vàlides les remissions genèriques a l'article del RGPD que els regula.

5.- MESURES DE RESPONSABILITAT ACTIVA

El RGPD estableix un catàleg de les mesures que els responsables, i en ocasions els encarregats, han d'aplicar per garantir que els tractaments que realitzen són conformes amb el Reglament i estar en condicions de demostrar-ho.

5.1.- Anàlisis de risc

El RGPD condiciona l'adopció de les **mesures de responsabilitat activa al risc que els tractaments puguin suposar per als drets i llibertats dels interessats**.

Es maneja el risc de dues maneres:

• En alguns casos, preveu que determinades mesures solament hauran d'aplicar-se quan el tractament suposi un alt risc per als drets i llibertats.

• En altres casos, les mesures hauran de modular-se en funció del nivell i tipus de risc que el tractament comporti.

Obligacions: Tots els responsables hauran de realitzar una valoració del risc dels tractaments que realitzin, a fi de poder establir què mesures han d'aplicar i com han de fer-ho.

El tipus d'anàlisi variarà en funció de:

- Els tipus de tractament.
- La naturalesa de les dades.
- El nombre d'interessats afectats.
- La quantitat i varietat de tractaments que una mateixa organització dugui a terme.

5.2.- Registre d'activitats de tractament

Responsables i encarregats hauran de mantenir un registre d'operacions de tractament en el qual es contingui la informació que estableix el RGPD i que contingui qüestions com:

- Nom i dades de contacte del responsable o corresponsable i del Delegat de Protecció de dades si existís.
- Finalitats del tractament.
- Descripció de categories d'interessats i categories de dades personals tractades.
- Transferències internacionals de dades.

Estan exemptes les organitzacions que emprin a menys de 250 treballadors, tret que el tractament que realitzin pugui comportar un risc per als drets i llibertats dels interessats, no sigui ocasional o inclogui categories especials de dades o dades relatives a condemnes i infraccions penals.

5.3.- Protecció de dades des del disseny i per defecte.

Es tracta de pensar en termes de protecció de dades des del mateix moment en què es dissenya un tractament, un producte o servei que implica el tractament de dades personals.

Des de l'inici, els responsables han de prendre mesures organitzatives i tècniques per integrar en els tractaments garanties que permetin aplicar de forma efectiva els principis del RGPD. Els responsables han d'adoptar mesures que garanteixin que solament es tractin les dades necessàries quant a la quantitat de dades tractades, l'extensió del tractament, els períodes de conservació i l'accessibilitat a les dades.

5.4.- Mesures de seguretat.

ABANS: El Reglament de Desenvolupament de la LOPD determinava amb detall i de forma exhaustiva les mesures de seguretat que havien d'aplicar-se segons el tipus de dades objecto de tractament. Les mesures del Reglament de la LOPD estaven basades gairebé exclusivament en el tipus de dades que es tractaven, amb alguna matisació relativa al context en què es duien a terme els tractaments.

ARA: En el RGPD, els responsables i encarregats establiran les mesures tècniques i organitzatives apropiades per garantir un nivell de seguretat adequat en funció dels riscos detectats en l'anàlisi prèvia. Demana que es prenguin en consideració més variables.

L'esquema de mesures de seguretat previst en el Reglament de Desenvolupament de la LOPD no seguirà sent vàlid de forma automàtica després de la data d'aplicació del RGPD.

En alguns casos els responsables podran seguir aplicant les mateixes mesures que estableix el Reglament de la LOPD si els resultats de l'anàlisi de riscos previ conclou que les mesures són realment les més adequades per oferir un nivell de seguretat adequat. En ocasions serà necessari completar-les amb mesures addicionals o prescindir d'alguna de les mesures.

5.5.- Notificació de “violació de seguretat de les dades”

El RGPD defineix les violacions de seguretat de les dades, més comunament conegudes com a “fallides de seguretat”, d'una forma molt àmplia, que inclou tot incident que ocasioni la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservats o tractats d'una altra forma, o la comunicació o accés no autoritzats a aquestes dades. Successos com la pèrdua d'un ordinador portàtil, l'accés no autoritzat a les bases de dades d'una organització (fins i tot pel seu propi personal) o l'esborrat accidental d'alguns registres constitueixen violacions de seguretat a la llum del RGPD i han de ser tractades com el Reglament estableix.

Quan es produeixi una violació de la seguretat de les dades, el responsable ha de notificar-la a l'autoritat de protecció de dades competent, tret que sigui improbable que la violació suposi un risc per als drets i llibertats dels afectats.

La notificació de la fallida a les autoritats ha de produir-se sense dilació indeguda i, si pot ser, dins de les 72 hores següents al fet que el responsable tingui constància d'ella.

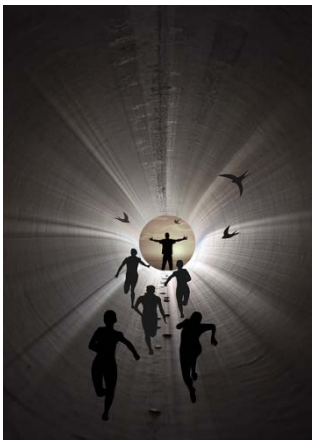
La notificació ha d'incloure un contingut mínim:

- La naturalesa de la violació
- Categories de dades i d'interessats afectats.
- Mesures adoptades pel responsable per solucionar la fallida.
- Si escau, les mesures aplicades per pal·liar els possibles efectes negatius sobre els interessats.

Els responsables han de documentar totes les violacions de seguretat.

En els casos en què sigui probable que la violació de seguretat comporti un alt risc per als drets o llibertats dels interessats, la notificació a l'autoritat de supervisió haurà de complementar-se amb una notificació dirigida a aquests últims.

L'objectiu de la notificació als afectats és permetre que puguin prendre mesures per protegir-se de les seves conseqüències. Per això, el RGPD requereix que es realitzi sense dilació indeguda, sense fer referència ni al moment en què es tingui constància d'ella ni tampoc a la possibilitat d'efectuar la notificació dins d'un termini de 72 hores. El propòsit és sempre que l'interessat afectat pugui reaccionar tan aviat com sigui possible.



A tenir en compte

- La valoració del risc de la fallida és diferent de l'anàlisi de riscos previ a tot tractament. Es tracta d'establir fins a quin punt l'incident, per les seves característiques, el tipus de dades als quals es refereix o el tipus de conseqüències que pot tenir per als afectats pot causar un dany en els seus drets o llibertats.

- Els danys poden ser materials o immaterials, i anar des de la possible discriminació dels afectats com a conseqüència del seu ús per qui ha accedit a ells de forma no autoritzada fins a usurpació d'identitat, passant per perjudicis econòmics o l'exposició pública de dades confidencials.

- Es considera que es té constància d'una violació de seguretat quan hi ha una certesa que s'ha produït i es té un coneixement suficient de la seva naturalesa i abast.

- La mera sospita que ha existit una fallida o la constatació que ha succeït algun tipus d'incident sense que es coneguin mínimament les seves circumstàncies no haurien de donar lloc, encara, a la notificació, atès que en aquestes condicions no seria possible, en la majoria dels casos, determinar fins a quin punt pot existir un risc per als drets i llibertats dels interessats.

- En casos de fallides que per les seves característiques poguessin tenir gran impacte, sí podria ser recomanable contactar amb l'autoritat de supervisió tan aviat com existeixin evidències que s'ha produït alguna situació irregular respecte a la seguretat de les dades, sense perjudici que aquests primers contactes puguin completar-se amb una notificació formal més completa dins del termini legalment previst.

- Pot haver-hi casos en què la notificació no pugui realitzar-se dins d'aquestes 72 hores, per exemple, per la complexitat a determinar completament el seu abast. En aquests casos, és possible fer la notificació amb posterioritat, acompanyant-la d'una explicació dels motius que han ocasionat el retard.

- La informació pot proporcionar-se de forma escalonada quan no sigui possible fer-ho al mateix moment de la notificació.

- El criteri d'alt risc ha d'entendre's en el sentit que sigui probable que la violació de seguretat ocasioni danys d'entitat als interessats. Per exemple, en casos en què es desvetlli informació confidencial, com a contrasenyes o participació en determinades activitats, es difonguin de forma massiva dades sensibles o es puguin produir perjudicis econòmics per als afectats.

La notificació als interessats no serà necessària quan:

• El responsable hagués pres mesures tècniques o organitzatives apropiades amb anterioritat a la violació de seguretat, en particular les mesures que facin ininteL·ligibles les dades per a tercers, com seria el xifrat.

• Quan el responsable hagi pres amb posterioritat a la fallida mesurades tècniques que garanteixin que ja no hi ha possibilitat que l'alt risc es materialitzi.

• Quan la notificació suposi un esforç desproporcionat, havent d'en aquests casos substituir-se per mesures alternatives com pot ser una comunicació pública.

5.6.- Avaluació d'impacte sobre la protecció de dades

Avaluació d'Impacte en la Protecció de les Dades Personals (EIPD) és, en essència, un exercici d'anàlisi dels riscos que un determinat sistema d'informació, producte o servei pot comportar per al dret fonamental a la protecció de dades dels afectats i, després d'aquesta anàlisi, afrontar la gestió eficaç dels riscos identificats mitjançant l'adopció de les mesures necessàries per eliminar-los o mitigar-los.

Els responsables de tractament hauran de realitzar una Avaluació d'Impacte sobre la Protecció de Dades (EIPD) amb caràcter previ a l'engegada d'aquells tractaments que sigui probable que comportin un alt risc per als drets i llibertats dels interessats.

El RGPD estableix un contingut mínim de les Avaluacions d'Impacte sobre la Protecció de Dades, encara que no contempla cap metodologia específica per a la seva realització

(L'AEPD va publicar en 2014 una Guia sobre aquestes Avaluacions que serà actualitzada i publicada durant el període transitori per incorporar les novetats del RGPD)

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf.

6.- ELS DRETS DELS INTERESSATS

El titular de **les dades personals** emmagatzemades en els fitxers de la meva empresa o entitat té una sèrie de **drets** pel que fa al tractament dels mateixos. Aquests drets són:

- Dret d'accés a les seves dades.
- Dret de rectificació de les seves dades.
- Dret de cancel·lació de les seves dades.
- Dret d'oposició al tractament.
- Els drets anteriorment citats es coneixen com a drets ARC (A accés, R rectificació, C cancel·lació i O oposició).
- Impugnació de valoracions.
- Consulta al Registre General.

Alguns d'aquests drets **suposen correlatius deures per a la meva empresa o entitat** com a responsable dels fitxers.

La meva empresa o entitat té l'obligació de facilitar l'exercici de tals drets per part de l'interessat.

Dret d'accés

L'afectat té dret a sol·licitar **a la meva empresa** o entitat, com a responsable del fitxer on s'emmagatzemen les seves dades, **que li informi** sobre quins són les dades emmagatzemades, la manera en què la meva empresa els ha obtingut i les cessions que la meva empresa hagi fet a terceres persones.

Aquest dret no és absolut i es podrà negar l'accés quan el dret ja s'hagi exercitat, per l'afectat, en els dotze mesos anteriors a la sol·licitud, tret que s'acrediti un interès legítim a aquest efecte o existeixi una norma que impedeixin al responsable del tractament revelar als afectats l'ús de les dades als quals es refereixi l'accés.

Rebuda la sol·licitud, si la meva empresa té dades de l'afectat en els seus fitxers, ha de **contestar-li en el termini d'1 mes** atenent l'exercici del dret d'accés.

Dret de rectificació

L'afectat pot sol·licitar a la meva empresa o entitat, com a responsable del fitxer, **que corregeixi o completi un o varis de les seves dades** que estiguin emmagatzemats en el fitxer de forma errònia o incompleta.

Té dret al fet que actualitzem dades com a canvis de domicili, o uns altres similars. La meva empresa té l'obligació de corregir o completar les dades en el **termini d'1 mes** des que l'afectat ha formulat la seva sol·licitud.

Dret de cancel·lació

L'interessat, al·legant una causa justificada, pot **sol·licitar a la meva empresa o entitat que les seves dades siguin excloses del fitxer**, revocant el consentiment que en el seu moment va atorgar perquè fossin incorporats al mateix. Pot ser total o parcial, per afectar a tots o només a part de les dades tractades en el nostre fitxer.

La meva empresa té l'obligació de fer efectiu el dret de cancel·lació en el **termini d'1 mes**, tret que el manteniment de les seves dades en el fitxer sigui necessari per al manteniment o compliment de la relació que li uneix amb la meva empresa o entitat.

Dret d'oposició

Consisteix en el **dret que tenen els titulars de dades**, quan el seu consentiment no sigui necessari per al tractament, **d'oposar-se al mateix** una vegada tinguin coneixement que s'ha produït. L'oposició pot ser total o parcial quant a les finalitats del fitxer en el qual les seves dades estan emmagatzemades.
En tal suposat, la meva empresa té l'obligació de cancel·lar les seves dades del fitxer, a la seva simple sol·licitud i sense despeses, al mateix moment en què es rebi el requeriment.

Impugnació de valoracions

L'afectat pot **impugnar els actes administratius o decisions privades** que impliquen una valoració del seu comportament, l'únic fonament del qual sigui un tractament de dades personals que ofereixi una definició de les seves característiques o personalitat.

És el cas, per exemple, de les tècniques de “scoring” en la contractació. Permeten valorar de forma automàtica si les característiques d'una persona s’adeqüen als requisits exigits per una empresa que li va a contractar.

Consulta al registre general.

Qualsevol persona pot dirigir-se al Registre General de Protecció de Dades amb la finalitat de conèixer l'existència de tractaments de les seves dades personals, les finalitats amb que es tracten i la identitat del responsable del fitxer on estan emmagatzemats.

El Registre General de Protecció de Dades és de consulta pública i gratuïta. Per a la meva empresa **suposa l'obligació correlativa d'inscriure els meus fitxers** en aquest registre.

El RGPD conté els ja tradicionals drets ARC i també alguns nous drets. A més, estableix condicions concretes sobre el procediment a seguir per atendre als interessats en l'exercici dels seus drets.

RGPD incorpora el **dret a l'oblit com un dret vinculat al dret de supressió, al dret a la limitació del tractament i al dret a la portabilitat:**

Dret a l’oblit

Els interessats tenen **dret a obtenir la supressió de les dades** ("dret a l'oblit"), quan:

- Les dades ja no són necessaris per a la finalitat per la qual es van recollir.
- Es revoca el consentiment en el qual es basava el tractament.
- L'interessat s'oposa al tractament.
- Les dades s'han tractat il·lícitament.
- Les dades s'han de suprimir per complir una obligació legal.
- Les dades s'han obtingut en relació amb l'oferta de serveis de la societat de la informació dirigida a menors.

Quan el responsable ha fet públics les dades personals i han de suprimir-se, ha d'adoptar mesures raonables per informar de la supressió els responsables que estan tractant les dades.

Es preveuen algunes excepcions a l'exercici d'aquest dret:

- L'exercici del dret a la llibertat d'expressió i informació.
- El compliment d'una obligació legal.
- L'existència de finalitats d'arxiu en interès públic, de recerca científica o històrica o finalitats estadístiques.
- La formulació, l'exercici o la defensa de reclamacions.

Dret a la limitació del tractament.

La limitació de tractament es presenta en el RGPD com un dret de les persones interessades. Per això, no s'ha de confondre amb el bloqueig de dades actualment existent en la legislació espanyola, encara que el fet que s'hagi inclòs com a nou dret no suposa, per si solament, que la figura del bloqueig desapareix.

La limitació de tractament suposa que, a petició de la persona interessada, no s'aplicaran a les seves dades personals les operacions de tractament que en cada cas correspondrien. La limitació es pot sol·licitar quan:

L'interessat ha exercit els drets de rectificació o oposició i mentre el responsable determina si escau atendre la sol·licitud.
El tractament és il·lícit, la qual cosa determinaria l'esborrat de les dades, però l'interessat s'oposa.
Les dades ja no són necessàries per al tractament, la qual cosa novament en determinaria l'esborrat, però l'interessat sol·licita la limitació perquè els necessita per formular, exercir o defensar reclamacions.
A aquest dret se li apliquen els mateixos terminis i procediments que en la resta de drets previstos en el RGPD.

Mentre duri la limitació, el responsable només pot tractar les dades afectades, més enllà de conservar-les, en els casos següents:

- Amb el consentiment de l'interessat.
- Per formular, exercir o defensar reclamacions.
- Per protegir els drets d'una altra persona física o jurídica.
- Per raons d'interès públic important de la Unió o de l'Estat membre corresponent.

Una conseqüència d'aquesta regulació és que impedeix una pràctica que de vegades se segueix i que consisteix a esborrar les dades quan s'exerceixen altres drets, com el d'accés, ja que impediria l'exercici del dret a la limitació del tractament.

Derecho a la portabilidad

El dret a la portabilitat de les dades és una forma avançada del dret d'accés, per la qual l'interessat té dret a rebre les dades personals que li afecten i que ha facilitat a un responsable del tractament en un format estructurat, d'ús comú i de lectura mecànica, i transmetre-les a un altre responsable, si es compleixen els requisits següents:

- El tractament està basat en el consentiment o en un contracte.
- El tractament es fa per mitjans automatitzats.
- L'interessat ho sol·licita respecte de les dades que ha proporcionat al responsable i que li concerneixen, inclosos les dades derivades de la pròpia activitat de l'interessat.

Això suposa que no és aplicable a les dades de terceres persones que un interessat hagi facilitat a un responsable. Tampoc s'aplicarà si l'interessat sol·licita la portabilitat de dades que li incumbeixen, però que han estat proporcionats al responsable per tercers.

Inclou el dret que les dades es transmetin directament de responsable a responsable, si és tècnicament possible.

¿ Com és el procediment per exercir els drets recollits pel nou reglament ?

Amb caràcter general, el RGPD exigeix als responsables que facilitin als interessats l'exercici dels seus drets. Aquest mandat suposa que els procediments i les formes per fer-ho han de ser visibles, accessibles i senzilles. El RGPD no estableix una manera concreta per exercir els drets, però sí requereix als responsables que possibilitin que les sol·licituds es presentin per mitjans electrònics, especialment quan el tractament s'efectua per aquests mitjans.

Aquesta obligació exigeix articular procediments que permetin fàcilment que les persones interessades puguin acreditar que han exercit els seus drets per mitjans electrònics, la qual cosa actualment en moltes ocasions no és viable.

El RGPD preveu també que l'exercici de drets ha de ser gratuït per a l'interessat. Aquest criteri de gratuïtat pot no seguir-se en els casos en què es formulen sol·licituds manifestament infundades o excessius, especialment per a repetitives; en aquests casos, el responsable pot cobrar un cànon que compensi els costos administratius d'atendre la petició, o bé negar-se a actuar. És el responsable qui ha de demostrar aquest caràcter infundat o excessiu. En tot cas, el cànon no pot implicar un ingrés addicional per al responsable, sinó que ha de correspondre al veritable cost de la tramitació de la sol·licitud.

El responsable ha d'informar a la persona interessada sobre les actuacions derivades de la seva petició en el termini d'un mes, que es pot ampliar dos mesos més quan es tracta de sol·licituds especialment complexes. Aquesta ampliació del termini es notificarà dins del primer mes. Si el responsable decideix no atendre la sol·licitud, informarà i motivar la negativa dins del termini d'un mes des que es va presentar.

D'acord amb el RGPD, els responsables han de prendre totes les mesures raonables per verificar la identitat dels afectats que sol·liciten accés i, en general, els afectats que exerceixen la resta de drets ARC.

El responsable que tracta una gran quantitat d'informació sobre un interessat pot demanar-li que especifiqui la informació al fet que es refereix la seva sol·licitud d'accés.

El responsable pot comptar amb la col·laboració dels encarregats per atendre l'exercici de drets dels interessats. Aquesta col·laboració es pot incloure en el contracte per encàrrec de tractament.

L'afectat al que es denegui, total o parcialment, l'exercici dels seus drets d'oposició, accés, rectificació o cancel·lació pot **posar-ho en coneixement de l'AGÈNCIA DE PROTECCIÓ DE DADES.**

S'inicia llavors un procediment per a l'atenció de l'exercici de la tutela, que acaba amb una resolució de la APD i **pot donar lloc a la imposició de sancions.**

Fundació Pere Tarrés

www.**peretarres**.org

Carolines - 10 | 08021 | Barcelona | Tel. 93 410 16 02 | formacio@peretarres.org

FUNDACIÓ
PERE TARRÉS