l'empresa)

Aspectes més destacats del nou Reglament General de Protecció de Dades

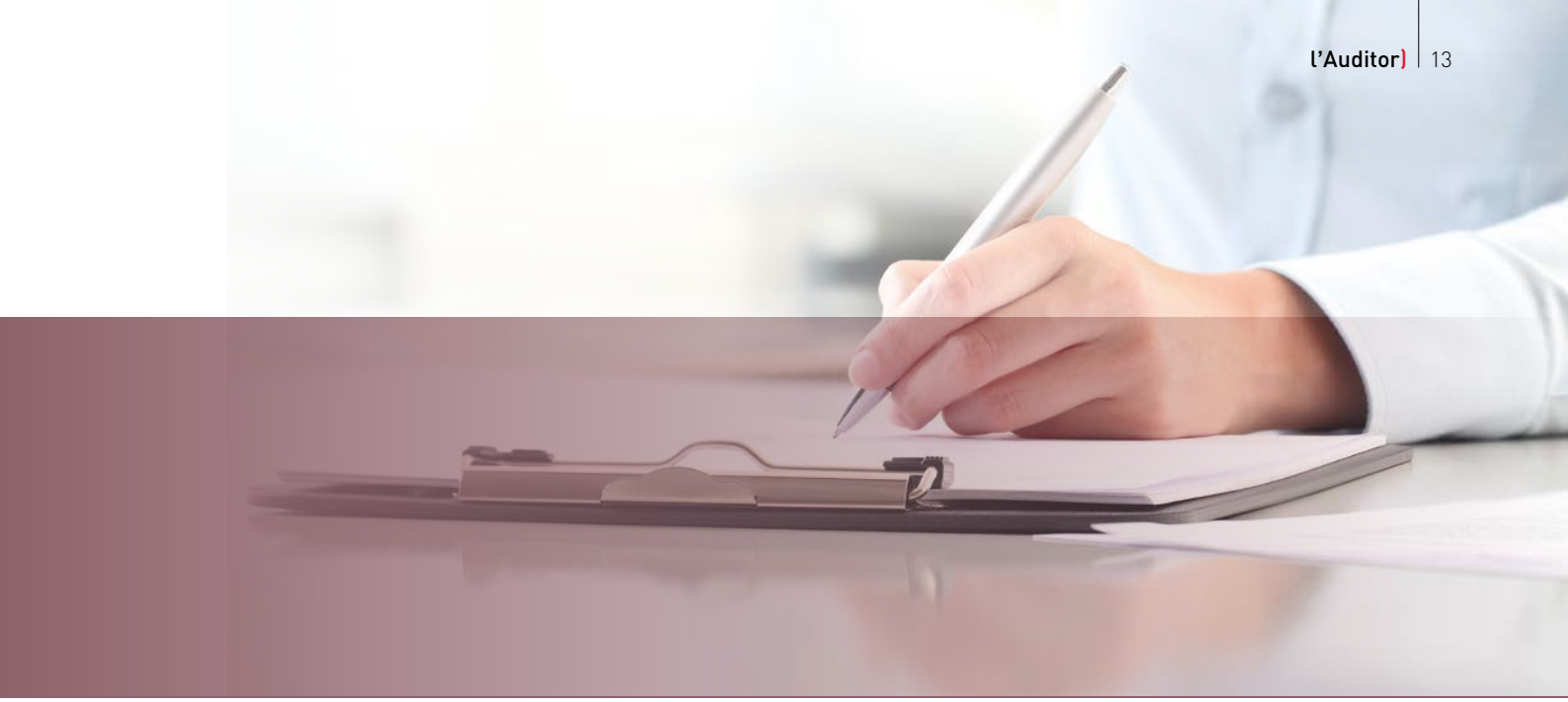
Juan Luis Casanova
Soci d'Audria Auditoria Consultoria, S.L.P.
i membre del Comitè tècnic

D'aquí a poques setmanes es posarà en marxa el nou Reglament General de Protecció de Dades (RGPD) que va entrar en vigor al maig de 2016 i que serà aplicable a partir del 25 de maig de 2018 a la Unió Europea (UE). Si bé aquesta nova norma serà aplicable a partir d›aquesta data en tots els Estats membres, sense necessitat de transposició, és necessari que els ordenaments nacionals s'actualitzin, sempre sense contradir allò que disposa l'RGPD. En aquest sentit, el mes de novembre passat, el Consell de Ministres va remetre a les Corts Generals el Projecte de Llei Orgànica de protecció de dades, que té per objecte adaptar la nostra legislació nacional al Reglament (UE) 2016/679 del Parlament Europeu i, per tant, substituir l'actual Llei Orgànica 15/1999.

Els auditors en l'exercici de la nostra professió processem de manera habitual dades personals dels nostres clients o empleats, com per exemple, el DNI, el domicili particular, la situació familiar, el nivell d'ingressos o el seu número de telèfon, per la qual cosa hem de fer una anàlisi de riscos amb la finalitat d'establir les mesures que siguin necessàries per garantir els drets i les llibertats de les persones i revisar els nostres procediments per assegurar-nos el compliment de les noves disposicions abans del 25 de maig.

ASPECTES MÉS DESTACATS DEL NOU RGPD

1 **OBTENCIÓ DEL CONSENTIMENT PER AL TRACTAMENT DE DADES**
El consentiment s'ha de donar mitjançant un acte afirmatiu clar que reflecteixi una manifestació de voluntat lliure, específica, informada i inequívoca de l'interessat d'acceptar el tractament de dades de caràcter personal que li concerneixen, com una declaració per escrit, inclusivament per mitjans electrònics, o una declaració verbal. Això podria incloure marcar una casella d'un lloc web a Internet, escollir paràmetres tècnics per a la utilització de serveis de la societat de la informació o qualsevol altra declaració o conducta que indiqui clarament en aquest context que l'interessat accepta la proposta de tractament de les seves dades personals. **Per tant, el silenci, les caselles ja marcades o la inacció no han de constituir consentiment**. El consentiment s'ha de donar per a totes les activitats de tractament fetes amb aquest o les mateixes finalitats. Si el tractament té diverses finalitats, ha de donar-se el consentiment per a totes.



2 DRETS DELS INTERESSATS. INFORMACIÓ I ACCÉS A LES DADES PERSONALS

El RGPD atorga a les persones físiques drets sobre les seves dades personals i estableix fórmules i mecanismes per sol·licitar i, si escau, obtenir gratuïtament l'accés a les dades personals i la seva rectificació o supressió, així com l'exercici del dret d'oposició.
El responsable del tractament també ha de proporcionar mitjans perquè les sol·licituds es presentin per mitjans electrònics, en particular quan les dades personals es tracten per mitjans electrònics. El responsable del tractament està obligat a respondre a les sol·licituds de l'interessat sense dilació indeguda, com a molt tard en el termini d'un mes, i a explicar-ne els motius en cas que no les atengués.

En concret, se'ls ha d'informar, entre d'altres, de les qüestions següents:

- La identitat i les dades de contacte del responsable i, si escau, del seu representant
- Les dades de contacte del delegat de protecció de dades, si escau
- Les finalitats del tractament a què es destinen les dades personals
- El termini durant el qual es conserven les dades personals
- El dret a sol·licitar al responsable del tractament l'accés a les dades personals i a la seva rectificació, supressió, limitació o oposició al seu tractament, així com el dret a la portabilitat de les dades
- L'existència del dret a retirar el consentiment en qualsevol moment
- El dret a presentar una reclamació davant d'una autoritat de control (Agència Espanyola de Protecció de Dades)

Dret d'accés de l'interessat

L'interessat (la persona física identificable) té dret a obtenir del responsable del tractament la confirmació de si s'estan tractant o no dades personals que li concerneixen i, en aquest cas, dret d'accés a les dades personals, les finalitats del tractament; les categories de dades personals de què es tracti, els destinataris als quals es van comunicar o s'han de comunicar les dades personals, el termini previst de conservació de les dades personals, el dret a sol·licitar del responsable la rectificació o supressió de les dades personals, el dret a presentar una reclamació davant una autoritat de control. Quan les dades personals no s'hagin obtingut de l'interessat, qualsevol informació disponible sobre el seu origen, l'existència de decisions automatitzades, inclosa l'elaboració de perfils, etc.

Dret de rectificació

L'interessat té dret a obtenir del responsable del tractament la rectificació de les dades personals inexactes que li concerneixin. Tenint en compte les finalitats del tractament, l'interessat té dret que es completin les dades personals que siguin incompletes, inclusivament mitjançant una declaració addicional.

Dret de supressió ("dret a l'oblit")

L'interessat té dret a obtenir del responsable del tractament la supressió de les dades personals que li concerneixin. El responsable està obligat a suprimir les dades personals quan aquestes dades ja no siguin necessàries en relació amb les finalitats per a les quals es van recollir, quan l'interessat retiri el consentiment en què es basa el tractament, si les dades personals s'han tractat il·lícitament, si les dades personals s'han de suprimir per al compliment d'una obligació legal que s'estableix en el Dret de la Unió o dels Estats membres, etc.

Dret a la limitació del tractament

L'interessat té dret a obtenir del responsable del tractament la limitació del tractament de les dades quan es compleixi alguna de les condicions següents:

- quan l'interessat impugni l'exactitud de les dades personals, durant un termini que permeti al responsable verificar-ne l'exactitud.

- quan el tractament sigui il·lícit i l'interessat s'oposi a la supressió de les dades personals i sol·liciti en lloc seu, la limitació de l'ús.
- quan el responsable ja no necessiti les dades personals per a les finalitats del tractament, però l'interessat les necessiti per a la formulació, l'exercici o la defensa de reclamacions, etc.

Quan el tractament de dades personals s'hagi limitat en virtut de l'apartat anterior, aquestes dades només poden ser objecte de tractament, amb excepció de la seva conservació, amb el consentiment de l'interessat o per a la formulació, l'exercici o la defensa de reclamacions.

Dret a la portabilitat de les dades
L'interessat té dret a rebre les dades personals que li incumbeixin, les que hagi facilitat a un responsable del tractament, en un format estructurat, d'ús comú i lectura mecànica, i a transmetre-les a un altre responsable del tractament sense que ho impedeixi el responsable al qual les hi hagués facilitat.

Dret d'oposició
L'interessat té dret a oposar-se en qualsevol moment, per motius relacionats amb la seva situació particular, que les dades personals que li concerneixin siguin objecte d'un tractament, inclosa l'elaboració de perfils. El responsable del tractament ha de deixar de tractar les dades personals, tret que acrediti motius legítims imperiosos per al tractament que prevalguin sobre els interessos, els drets i les llibertats de l'interessat, o per a la formulació, l'exercici o la defensa de reclamacions. Quan l'interessat s'oposi al tractament amb finalitats de màrqueting directe, les dades personals deixaran de tractar-se per a aquestes finalitats.

Dret a la Transparència de la informació
El responsable del tractament ha de prendre les mesures oportunes per facilitar a l'interessat tota la informació relativa a les seves dades personals i al tractament, en forma concisa, transparent, intel·ligible i de fàcil accés, amb un llenguatge clar i senzill, en particular qualsevol informació dirigida específicament a menors (nens en la terminologia de l'RGPD). La informació s'ha de facilitar per escrit o per altres mitjans, inclusivament, si escau, per mitjans electrònics. Quan ho sol·liciti l'interessat, la informació es pot facilitar verbalment, sempre que es demostri la identitat de l'interessat per altres mitjans.

3 AVALUACIÓ DE L'IMPACTE DEL TRACTAMENT DE LES DADES PERSONALS

En les organitzacions en què sigui probable que les operacions de tractament comportin un risc alt per als drets i llibertats de les persones físiques, ha d'incumbir al responsable del tractament la realització d'una avaluació d'impacte relativa a la protecció de dades (EIPD), que avaluï, en particular, l'origen, la naturalesa, la particularitat i la gravetat d'aquest risc. El resultat de l'avaluació s'ha de tenir en compte quan es decideixin les mesures adequades que s'hagin de prendre, amb la finalitat de demostrar que el tractament de les dades personals està d'acord amb el Reglament. Si una (EIPD) avaluació d'impacte relativa a la protecció de dades mostra que les operacions de tractament comporten un risc alt que el responsable no pot mitigar amb mesures adequades en termes de tecnologia disponible i costos d'aplicació, s'ha de consultar a l'autoritat de control abans del tractament. L'anàlisi i la gestió de riscos són procediments que permeten a les organitzacions fer un diagnòstic sobre els riscos per als tractaments de dades personals i, de vegades, aportar prou informació per decidir si cal dur a terme o no una Avaluació d'Impacte en Protecció de Dades. L'AEPD disposa de Guies d'Anàlisi de Risc i Avaluació d'Impacte en la Protecció de Dades Personals.

4 VIOLACIÓ DE LA SEGURETAT DE LES DADES PERSONALS

En cas de violació de la seguretat de les dades personals, el responsable del tractament l'ha de notificar a l'autoritat de control competent, com a molt tard 72 hores després que n'hagi tingut constància, tret que sigui improbable que aquesta violació de la seguretat constitueixi un risc per als drets i les llibertats de les persones físiques. Si la notificació a l'autoritat de control no té lloc en el termini de 72 hores, ha d'anar acompanyada de la indicació dels motius de la dilació.

5 DELEGAT DE PROTECCIÓ DE DADES

Segons el RGPD, les empreses i els tercers que processin dades personals en nom seu han de designar un delegat de protecció de dades (DPD) sempre que:

- es tracti d'una autoritat o organisme públic, excepte els tribunals que actuïn en exercici de la seva funció judicial,
- les activitats principals de l'empresa o el tercer consisteixin en l'observació d'interessats a gran escala; o
- les seves activitats principals consisteixin en el tractament a gran escala de dades personals sensibles, com les dades relatives a condemnes o infraccions penals.

El projecte de Llei Orgànica de protecció de dades (en tramitació), amplia la llista d'entitats que ha de nomenar un delegat de Protecció de Dades.

El DPD s'ha de nomenar atenent a les seves qualificacions professionals i, en particular, al seu coneixement de la legislació i la pràctica de la protecció de dades. Tot i que no ha de tenir una titulació específica, en la mesura en què

entre les funcions del DPD s'inclogui l'assessorament al responsable o encarregat en tot allò relatiu a la normativa sobre protecció de dades, els coneixements jurídics en la matèria són, sens dubte, necessaris, però també cal comptar amb coneixements aliens a l'estrictament jurídic, com per exemple en matèria de tecnologia aplicada al tractament de dades o en relació amb l'àmbit d'activitat de l'organització en la qual el DPD exerceix la seva tasca.

L'AEPD, en col·laboració amb l'Entitat Nacional d'Acreditació, disposen d'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 DPD reuneixen les qualificacions professionals i els coneixements que es requereixen. La certificació no és un requisit indispensable per a l'accés a la professió, és només una opció a la disposició de responsables i encarregats per tal de facilitar la selecció dels professionals.

No és imprescindible que el DPD sigui un empleat directe, sinó que pot exercir aquesta funció en el marc d'un contracte de serveis i pot desenvolupar la seva funció a temps parcial o complet. Les dades de contacte del DPD s'han de fer públiques i s'han de comunicar a les autoritats de supervisió competents.

6 REGISTRE DE LES ACTIVITATS DE TRACTAMENT

Les organitzacions que habitualment duguin a terme un tractament de dades de risc per a la privadesa dels interessats o tractin dades sensibles, han de portar un registre de les activitats de tractament efectuades sota la seva responsabilitat. Aquest registre ha de contenir, entre altres qüestions, informació relativa a les dades de contacte del responsable, les finalitats del tractament, una descripció de les categories de les dades personals, els destinataris de les dades, els terminis previstos per a la supressió, les mesures tècniques i organitzatives de seguretat adoptades.
Aquestes obligacions no s'apliquen a cap empresa ni organització que tingui menys de 250 empleats, tret que el tractament que dugui a terme pugui comportar un risc per als drets i les llibertats dels interessats, no sigui ocasional, o inclogui categories especials de dades personals com: origen ètnic, opcions polítiques o religioses, afiliació sindical, dades relatives a la salut o dades relatives a la vida sexual o l'orientació sexual d'una persona física, dades personals relatives a condemnes i infraccions penals, etc.

7 PROTECCIÓ DE DADES DES DEL DISSENY I PER DEFECTE

Aquest principi defineix la necessitat que el responsable del tractament apliqui mesures tècniques i organitzatives adients per tal de garantir i poder demostrar que el tractament està d'acord amb el Reglament. Aquest concepte 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 explícitament de quina manera aplicaran les mesures que preveu el RGPD, i han d'assegurar que aquestes mesures són les adequades per complir amb aquest i que poden demostrar-ho davant els interessats i davant les autoritats de supervisió. Aquest tipus de mesures pretenen reflectir l'enfocament de responsabilitat proactiva. Es tracta d'implementar mesures 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.

El responsable del tractament ha d'aplicar les mesures tècniques i organitzatives adients per tal de garantir que, per defecte, només siguin objecte de tractament les dades personals necessàries per a cadascuna de les finalitats específiques del tractament. Aquesta obligació s'ha d'aplicar en relació amb la quantitat de dades tractades, l'extensió del tractament, els períodes de conservació i l'accessibilitat a les dades.

8 SANCIONS

L'entrada en vigor del Reglament General de Protecció de Dades (RGPD), incrementa significativament les sancions que se'n deriven de l'incompliment.

A tall d'exemple, podem dir que són objecte de sanció (entre d'altres) les conductes següents:

- No atendre els drets dels interessats (accés, rectificació, oposició, portabilitat, dret a l'oblit, etc.)
- Les cessions de dades a tercers sense consentiment de l'interessat
- El tractament de dades per a finalitats diferents de les autoritzades
- Ignorar les violacions de les mesures de seguretat
- Etc.

Depenent de l'article del Reglament General de Protecció de Dades que s'hagi vulnerat, les infraccions s'han de sancionar amb multes administratives que van dels 10 milions als 20 milions d'euros com a màxim o, en tractar-se d'una empresa, d'una quantia equivalent al 2 % o al 4% com a màxim del volum de negoci total anual global de l'exercici financer anterior, i s'optarà per la de més quantia. A més de les multes administratives, el reglament preveu que les sancions puguin implicar també la prohibició del tractament de dades o la suspensió de les transferències internacionals de dades.