MANUAL-GUIA **SOBRE IMPACTES DEL REGLAMENT (UE) DE PROTECCIÓ DE DADES EN ELS ENS LOCALS**

Rafael Jiménez Asensio.
Consultor "Estudio Sector Público SLPU": Coordinació i redacció del document-base.

Ascen Moro.
Responsable de la Unitat de Gestió del Coneixement i Qualitat de l'Ajuntament de Sant Feliu de Llobregat

Han col·laborat en l'elaboració de la Guia: **Josep Betriu**, lletrat; **Irati Labaka Garmendia**, Estudio Sector Público; **Albert Guilera**, lletrat; **Estela Ribes Caballer**, politòloga; i **Alba Sánchez**, lletrada.

FEDERACIÓ DE MUNICIPIS DE CATALUNYA

ACM Associació Catalana de Municipis

Edita

Federació de Municipis de Catalunya
Via Laietana 33, 6è 1a. 08003 Barcelona

Associació Catalana de Municipis
Carrer de València, 231, 08007 Barcelona

Coordinació general
Juan Ignacio Soto Valle
Marc Pifarré i Estrada

Direcció acadèmica
Rafael Jiménez Asensio

Autors
Rafael Jiménez Asensio
Ascen Moro

Col·laboradors
Josep Betriu
Irati Labaka Garmendia
Albert Guilera
Estela Ribes Caballer
Alba Sánchez

Equip tècnic
Laura Gálvez
Mercè Canals
Elisabet Pérez

Disseny i maquetació
www.lacuinagrafica.com

ISBN 78-84-87286-61-2

ÍNDEX

PRESENTACIÓ		05
1. LÍNIES-FORÇA DEL NOU MARC NORMATIU DE LA UE EN MATÈRIA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL	Per què una nova regulació europea?	07
	Quins són els motius pels quals s'ha derogat la Directiva de 1995 i s'ha aprovat el Reglament de 2016?	07
	El nou marc normatiu de l'RGPD com a canvi de paradigma	08
2. QÜESTIONS GENERALS DE L'RGPD. ALGUNES NOVETATS SOBRE PRINCIPIS I DRETS	Introducció. Algunes claus per a la comprensió de l'RGPD.	08
	Quin és l'objecte de l'RGPD?	09
	S'aplica l'RGPD íntegrament als governs locals i a les seves entitats del sector públic?	10
	El nou concepte de "protecció de dades" i altres definicions	10
	Quins són els principis que s'han de tenir en compte en el tractament de dades personals?	11
	Quina és la nova configuració del "consentiment" en l'RGPD?	12
	Els tractaments de "categories especials"	13
	Quins drets garanteix l'RGPD a l'"interessat"?	13
	Quin és el nou marc normatiu de la informació i com afecta les entitats locals?	14
	Dret d'accés	16
	Dret de rectificació i supressió ("Dret a l'oblit")	17
	Dret a la limitació del tractament	17
	Dret a la portabilitat de les dades	17
	Dret d'oposició i decisions individuals automatitzades	18
	Limitacions	18
3. NOU SISTEMA INSTITUCIONAL I DE GESTIÓ DE PROTECCIÓ DE DADES EN L'ADMINISTRACIÓ PÚBLICA.	Introducció	18
	Responsables de tractament i encarregats de tractament: les seves peculiaritats aplicatives en l'àmbit del govern local	19
	Registre de les activitats de tractament	23
	Seguretat de les dades personals	24
	Anàlisi de riscos	25
	Avaluació d'impacte sobre la protecció de dades	27
	Delegat de protecció de dades	31
	Codis de conducta i mecanismes de certificació	35
	Autoritats de control independents: idea general	37
	Règim de responsabilitats i sancions: idea general. Aplicació al sector públic	39
	Altres qüestions: Situacions específiques de tractament.	42
	Final	43
BONA PRÀCTICA	Ajuntament de Sant Feliu de Llobregat: La seguretat integral i el nou model organitzatiu. Els reptes d'adequació a l'RGPD	44
DOSSIER DE DOCUMENTACIÓ		50

LA NECESSITAT DE REGULACIÓ EN MATÈRIA DE DADES PERSONALS

"Hay una cosa cierta al menos y es que también en este caso lo que se impone es la palabra regulación frente a una mercantilización y una desregulación del mundo sin equivalente alguno en la historia de la humanidad"

(Luc Ferry, La revolución transhumanista. Cómo la tecnología y la uberización del mundo van a transformar nuestras vidas, Alianza Editorial, 2017, pàg.154)

ARRIBA TARD?

"No es de extrañar que Alphabet (Google) ya no hurgue en nuestros correos electrónicos personales para mostrarnos anuncios personalizados: ya sabe todo de cada uno de nosotros y puede prescindir de más información (...) Es decir, en la medida en que el entorno normativo se vuelva más problemático y/o el mercado publicitario se desacelere (...) la compañía tendría un modelo de negocio muy robusto: vender 'servicios inteligentes' (IA), tanto a ciudadanos como a gobiernos"

(Evgeny Morozov, Capitalismo "Big Tech" ¿Welfare o neofeudalismo digital? Enclave, 2018, pàg. 23-24)

LES TASQUES PENDENTS

"Como los malos estudiantes, la mayoría de empresas españolas (y no digo nada de la Administración) no han hecho los deberes y ahora se acuerdan de Santa Bárbara, o de Santo Dato, cuando ya se escuchan los primeros truenos"

(Borja Adsuara Varela. Protección de Datos: Quedan solo cuatro meses para ponerse al día, Retina, enero 2018)

PRESENTACIÓ

La finalitat de la present Guia és oferir als operadors del món local, tant polítics com empleats públics, així com també a la ciutadania que es relaciona amb aquest nivell de govern, un manual bàsic sobre quines són les novetats més importants del Reglament 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (en endavant RGPD), en el que poden estimar-se quins són els impactes més rellevants que afecten els ens locals catalans i, així mateix, les entitats del seu sector públic vinculades, dependents o adscrites. En qualsevol cas, donat l'àmbit d'aplicació de l'RGPD, el que aquí segueix pot ser aplicat no solament als ens locals catalans, sinó a qualsevol govern local i, amb les modulacions que siguin procedents, també a altres administracions públiques territorials o ens del seu sector públic.

L'enfocament d'aquest breu treball és predominantment explicatiu. Es pretén que el lector no informat o escassament documentat sobre aquesta nova realitat normativa, comprengui quin és l'abast d'aquest marc regulador i quins seran els seus efectes aplicatius a partir del 25 de maig de 2018. El tractament d'aquest tema es fa mitjançant una anàlisi sistemàtica de l'RGPD on s'intercalen alguns documents d'interès (preferentment de les autoritats de control o del grup de treball de l'article 29), així com s'exposen algunes idees-força i altres recomanacions o opinions, que el temps haurà de contrastar.

Per tant, abans de precisar el seu contingut convé avançar tot el que la guia no és. En primer lloc, no es tracta d'una guia per a especialistes o persones que treballen en l'àmbit de la protecció de dades, encara que algunes de les qüestions que es tracten en aquest text puguin interessar o servir-los, si escau, d'orientació o informació addicional. En segon lloc, tampoc és una guia merament aplicativa (un enfocament seguit recentment pel decàleg publicat per la FEMP (encara que l'enllaç, després d'algun temps actiu, s'havia desactivat fa uns dies) o pel document recentment publicat per l'AEPD titulat *Protecció de Dades i Administració Local* i, particularment, per altres diferents i importants documents elaborats, ja sigui conjuntament o individualment, tant per apdCAT, com per l'AEPD o l'AVPD, recollides per l'annex documental d'aquest manual-guia).

Així mateix, no vol dir que no sigui d'utilitat el seu ús o consulta, ja que també s'incorporaran alguns consells puntuals sobre com aplicar determinats aspectes de la nova regulació als ens locals, incorporant diferents quadres per determinar quines mesures i protocols cal adoptar en la implantació d'aspectes rellevants del nou marc normatiu, com ara el registre de les activitats de tractament, l'anàlisi de riscos, l'avaluació d'impacte o el procés de designació de la figura del delegat de protecció de dades, per portar a col·lació quatre exemples d'indubtable transcendència per al funcionament del nou model de gestió de dades personals en les administracions locals.

Per tant, aquest manual-guia pretén ser una eina bàsicament pedagògica que faciliti la introducció a aquest nou model institucional i de gestió de dades personals i, així mateix, la seva comprensió, ja que sens dubte l'RGPD representa un notable **canvi de paradigma** en la forma i manera de comprendre i aplicar aquesta qüestió en l'àmbit local de govern o en qualsevol organització de caràcter públic.

En tot cas, encara que el present treball només s'ocupa de l'RGPD, es recolliran també de forma addicional i amb fins merament informatius (i un caràcter òbviament provisional) algunes referències puntuals al text del Projecte de llei orgànica de protecció de dades de caràcter personal (PLOPD), actualment en tramitació a les Corts Generals. Quan aquest text s'aprovi definitivament i sigui publicat en el "BOE" caldrà tornar a redefinir alguns aspectes puntuals d'aquesta guia.

Donada la naturalesa de l'instrument normatiu escollit (reglament de la Unió Europea), la posició aquesta vegada de la LOPD serà, a diferència de l'anterior, molt més vicarial o complementària. Certament, l'RGPD remet a més de cinquanta supòsits a què "les seves normes siguin especificades o restringides pel dret dels estats membres", però l'RGPD amb caràcter general té primacia aplicativa i entra en una sèrie de detalls en la regulació que la LOPD només podrà reenviar al que estableix el reglament.

Per tant, davant de la situació anterior, **l'operador** polític, directiu o tècnic **haurà d'actuar a partir d'aquest nou marc amb un binomi normatiu que haurà de consultar en paral·lel: RGPD i LOPD** (així com els reglaments que la desenvolupen). Així, no cal estranyar-se que aquest últim text (l'actual PLOPD) dugui a terme remissions constants a articles del mateix RGPD. El règim jurídic de protecció de dades personals descansarà, així, sobre dues "pantalles normatives" que s'han de visualitzar conjuntament: RGPD i LOPD. No hi haurà, ni tampoc es preveu, una norma que sintetitzi aquesta regulació.

El contingut de la present guia és molt senzill d'explicar.

La part central és una mena de manual explicatiu dels trets principals de la nova normativa i dels seus hipotètics impactes sobre els governs locals. Aquesta part s'estructura en tres grans eixos:

- El primer analitza **la transformació radical que s'ha produït en el model de protecció de dades de caràcter personal.**
- El segon s'ocupa de **les qüestions generals** que tracta el Reglament: especialment, **principis i drets**; amb un enfocament predominant cap a la ciutadania, però també a l'Administració que ha de tractar aquestes dades.
- I el tercer posa el focus d'atenció en els elements centrals del **nou model institucional i de gestió de protecció de dades personals** i la seva aplicació sobre els governs locals.

No es tractaran en aquesta guia, almenys directament, aquells aspectes que, en principi, incideixen menys directament sobre l'actuació dels governs locals. Per exemple, no s'aborda un tractament específic del capítol V (transferències de dades personals a tercers països

o organitzacions internacionals) o del VII (cooperació i coherència), entre d'altres temes, sense perjudici que totes aquestes previsions normatives s'han de tenir completament en compte en el tractament de dades personals per part del sector públic, més encara en un entorn de globalització de les dades i d'encreuament permanent d'informació.

Cal agrair, en aquest sentit, les aportacions o suggeriments que al contingut inicial ha dut a terme el meu bon amic Iñaki Vicuña, director del CENDOJ (Consell General del Poder Judicial) i, en el seu dia, també director de l'Agència Basca de Protecció de Dades, així com a n'Ascen Moro de l'Ajuntament de Sant Feliu de Llobregat. En tot cas, les errades o omissions només es poden imputar a qui ha estat l'encarregat de redactar el document-base.

Així mateix, **la guia conté una anàlisi de cas o bona pràctica. Es tracta d'exposar el que ha estat i el que serà la gestió de la protecció de dades de caràcter personal a l'Ajuntament de Sant Feliu de Llobregat (***La seguretat integral i el nou model organitzatiu. Els reptes d'adequació a l'RGPD*). **Aquesta part ha estat elaborada per la persona responsable de la matèria en l'esmentat Ajuntament.** Sens dubte, **Sant Feliu de Llobregat és un dels municipis catalans amb un desenvolupament digital i de seguretat de dades més rellevant,** fins al punt que el seu model de gestió ha estat objecte d'anàlisi en alguns llibres i premiat en diferents fòrums de gestió pública i innovació. D'aquí la seva importància per tractar-la en aquesta guia. El que ha fet i el que es proposi fer pot ser pres com un camí per a unes altres organitzacions locals.

I, en fi, la guía és un treball col·lectiu d'un equip que s'anuncia al principi i es tanca amb un breu dossier de documentació molt selectiu, on es pretenen recollir una sèrie de referències jurisprudencials, doctrinals i documentals, que puguin ajudar a l'operador, sigui polític o tècnic, *per saber-ne més* o completar algunes de les qüestions que succintament es tracten en el present text.

NOTA: *En aquesta guia les referències a l'RGPD es fan al text oficial editat en castellà. Hi ha una versió traduïda al català (sense caràcter oficial) realitzada per l'Autoritat Catalana de Protecció de Dades: http://apdcat.gencat.cat/ca/documentacio/RGPD/textos_normatius/*

Així mateix, algunes referències a documents publicats per l'AEPD, especialment l'últim ("Protecció de Dades i Administració Local"), en tant que no tenen versió oficial traduïda al català, s'ha preferit mantenir la redacció inicial en castellà. Veure el document citat: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2018/notas_prensa/news/2018_04_03-ides-idphp.php

1. LÍNIES-FORÇA DEL NOU MARC NORMATIU DE LA UE EN MATÈRIA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

Per què una nova regulació europea?

La necessitat objectiva de la nova regulació europea en matèria de protecció de dades de caràcter personal sorgeix del context tecnològic i de la seva evolució en les dues últimes dècades. En efecte, en els anys transcorreguts des de 1995 (data d'aprovació de la Directiva) fins a 2016 (data d'entrada en vigor del Reglament) la digitalització i la revolució tecnològica, així com la globalització de les dades, ha generant nous i importants reptes per a la protecció de les dades personals i, en particular, per als drets i llibertats dels ciutadans. I no sabem amb certesa què passarà en un futur immediat, encara que ho intuïm. Innombrables incògnites, incerteses i certes perplexitats envolten el desenvolupament de l'automatització, de la intel·ligència artificial i el Big Data (per no parlar dels ordinadors computacionals, que anuncien la fi de la privacitat) a escala encara desconeguda.

L'acceleració dels processos tecnològics i el seu impacte sobre les dades personals és, avui dia, una realitat incontestable, que anirà creixent cada vegada més, per la qual cosa aquesta nova regulació no només es dicta per afrontar els reptes del present, sinó especialment per fer front als grans desafiaments del futur en matèria de protecció de dades i de garantia dels drets i llibertats dels ciutadans, àmbits que en aquests moments són objecte d'una erosió no coneguda fins ara. El risc que es corre és que arribi tard o que aviat es quedi curta, sobretot per les dificultats d'adaptació que el marc regulador europeu presenta.

La manipulació de dades personals amb fins absolutament espuris (recordeu el recent cas de *Cambridge Analytica*) afecta principalment les grans companyies tecnològiques, però adverteix clarament d'una tendència ja fortament arrelada de mal ús de les dades personals per les grans companyies tecnològiques (en règim de quasi monopoli global) i empreses d'intermediació. En aquest accelerat context, el paper del sector públic i, particularment, de l'administració local, adquireix un paper de gran importància per tal de preservar els drets i llibertats de la ciutadania. La protecció de les dades personals que maneja quotidianament qualsevol nivell de govern es transforma en un repte d'alt valor democràtic.

La idea es troba perfectament expresada en el considerant 6 de l'RGPD: *"La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales"*

Quins són els motius pels quals s'ha derogat la Directiva de 1995 i s'ha aprovat el Reglament de 2016?

La derogació de la Directiva 96/45/CE i la seva substitució per l'RGPD no és una operació normativa menor. El canvi d'instrument regulador obeeix a raons de context i de la necessitat objectiva d'establir un reglament que, com és sabut, té un abast general, és obligatori en tots els seus elements i és directament aplicable.

La seva entrada en vigor es va produir al cap de vint dies des de la seva publicació en el DOUE, però la seva plena aplicabilitat es produeix a partir del 25 de maig de 2018 (article 99 RGPD).

En els considerants 9 a 13 de l'RGPD s'expliciten quins han estat els motius que han justificat el canvi d'instrument normatiu. Entre els que cal fer referència als següents:

- L'aplicació de la Directiva 1995 ha estat fragmentària i desigual, mentre que els riscos per a la protecció de dades són cada vegada més grans
- Es vol garantir un nivell uniforme i elevat de protecció de dades personals, i que sigui més equivalent en tots els estats membres. Es pretén assolir una aplicació de les normes de protecció de dades coherent i homogènia
- La protecció efectiva de les dades personals exigeix reforçar les obligacions de les persones encarregades del seu tractament, reconèixer poders equivalents per supervisar i garantir el seu compliment, així com l'establiment d'unes infraccions que castiguin amb sancions equivalents
- Hi ha base jurídica per a la seva regulació a l'article 16, 2 del TFUE. Tot i que el dret fonamental ja estava recollit (després traslladat al TFUE) en l'article 8 de la Carta de Drets Fonamentals de la Unió Europea

- Era, per tant, necessari regular aquesta matèria per un Reglament que proporcionés seguretat jurídica i transparència

El nou marc normatiu de l'RGPD com a canvi de paradigma

Aquest punt requereix un desenvolupament una mica més detingut. En efecte, la nota distintiva de l'actual marc normatiu (RGPD-futura LOPD) davant del vigent fins ara (Directiva-LOPD) resideix en transitar **des d'un model reactiu a un model proactiu o centrat en l'"enfocament de riscos".**

En certa mesura es pot afirmar que es trasllada a la protecció de dades de caràcter personal (encara que amb algunes limitacions, segons es veurà) *la política de compliance*, en què **la dimensió preventiva o anticipadora és una de les claus de volta del model que es pretén construir.**

Com s'ha vingut reconeixent, també per l'AEPD, s'ha produït un **autèntic canvi de paradigma** en la manera de gestionar les dades personals amb innegables conseqüències.

En aquesta lògica troben ple sentit diferents instruments o institucions que s'articulen dins del que es podria denominar com **un nou model institucional i de gestió de la protecció de dades en les organitzacions públiques**, que descansa principalment sobre els següents eixos de nova configuració:

1. Nou rol o nou marc de responsabilitats del responsable i de l'encarregat de tractament de dades
2. Registre de les activitats de tractament
3. Obligacions específiques vinculades amb la seguretat (*breach data*)
4. Anàlisi de riscos en el tractament
5. Avaluació d'impacte de les operacions de tractament
6. Implantació de la figura del delegat de protecció de dades (preceptiva en les administracions públiques)
7. Codis de conducta i mecanismes de certificació
8. Reforçament del paper de les autoritats de control (adpCAT/AEPD/AVPD)

No acaben aquí els elements d'aquesta nova arquitectura del model institucional i de gestió de protecció de dades, però aquests aspectes s'abordaran puntualment en altres passatges d'aquesta guia.

En qualsevol cas, aquest nou enfocament ja té alguns impactes evidents. Per exemple:

- Decau l'obligació de notificar a les autoritats de control l'existència de fitxers automatitzats
- Perd sentit, amb carácter general, la diferenciació entre nivells de protecció alt, mitjà i baix, que estableix la normativa en vigor. (vegeu, el que s'exposa més endavant: "Mesures de Seguretat")

IDEA-FORÇA:

Ante la constante evolución tecnológica y los procesos de transformación digital que sufren las actividades de tratamiento de datos personales, la reforma de la regulación de protección de datos supone un cambio del modelo tradicional para afrontar las medidas que garantizan la protección de datos personales hacia un nuevo modelo más dinámico, enfocado en la gestión continua de los riesgos potenciales asociados al tratamiento desde su diseño"

(AEPD, Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD)

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2018/notas_prensa/news/2018_02_28-ides-idphp.php

2. QÜESTIONS GENERALS DE L'RGPD. ALGUNES NOVETATS SOBRE PRINCIPIS I DRETS

Introducció. Algunes claus per a la comprensió de l'RGPD

En un manual-guia sobre l'impacte de l'RGPD a les entitats locals no pot faltar un tractament, encara que sigui epidèrmic, del que aquí s'anomena com "Qüestions Generals", amb especial atenció a les novetats sobre "principis" i "drets", algunes d'elles amb particular incidència en el quefer quotidià de les administracions locals quan tractin dades personals.

En tot cas, l'Administració Local es caracteritza per la seva proximitat a la ciutadania. I no s'ha de descartar que, també en aquesta matèria de protecció de dades personals, les autoritats locals i els seus agents hagin de dur a terme una tasca de difusió i sensibilització entre la ciutadania, complementària a la realitzada per les autoritats de control, sobre quins són els drets nous que les persones físiques tenen, també en relació amb el tractament de dades personals que es duguin a terme per les organitzacions públiques. La perspectiva del ciutadà és important també en aquest cas, especialment en administracions públiques prestadores de serveis.

Així, **no es pot oblidar mai que l'RGPD té per objecte la protecció de les persones físiques pel que fa als seus drets fonamentals i llibertats públiques en el seu conjunt**, no només (encara que també) es refereix al dret a la protecció de les seves dades personals, sinó especialment

quan fa referencia a la lesió d'aquest últim, ja que es poden menyscabar profundament l'exercici i gaudi de la resta de drets i llibertats. En aquest punt la realitat quotidiana ens mostra que aquesta afectació general és cada dia més real i profunda. Sota aquest punt de vista no és indiferent afirmar que **la protecció de dades personals és, avui dia, una batalla per l'estat democràtic i pel sistema de drets fonamentals assentats durant més de dos segles en els països occidentals.**

Algunes claus per a la comprensió d'aquest segon apartat es troben en els considerants de l'RGPD. Vegem succintament determinades referències i, en tot cas, es pot acudir a la lectura íntegra dels mateixos per a una major comprensió de la regulació que s'examina.

- ***A què s'apliquen els principis de la protecció de dades?*** (considerant 26):
    - "Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable". També a les dades "seudonimitzades"
    - Però no a la informació anònima, entesa com aquella ""que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable o deje de serlo" (vegeu: article 2.2, a quins tractaments no s'aplica l'RGPD)
- ***Principis*** (considerant 39):
    - " Todo tratamiento de datos debe ser lícito y leal"
    - El principi de transparència " exige que toda información y comunicación relativa al tratamiento de datos sea fácilmente accesible y fácil de entender y que se utilice un lenguaje sencillo y claro"
    - Els fins del tractament han de ser explícits i legítims i determinar-se en el moment de la seva recollida
    - S'ha de garantir que es limitin a un mínim estricte el termini de conservació de les dades (incorporar terminis per a la seva supressió o revisió periòdica")
- ***Nou règim jurídic del consentiment*** (considerants 32, 40 a 44):
    - "El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca"
    - Així, a partir de l'RGPD, ha de quedar clar que "las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos". (considerant 32).
    - Consentiment o Base jurídica legítima: " Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho". Es tracta d'un aspecte clau, especialment en el sector públic
    - Quan el tractament es porta a terme amb el consentiment de l'interessat: "El responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento" (vegeu les exigències en el considerant 42)
    - Així mateix, és important tenir en compte les garanties del consentiment exigides quan el tractament el duu a terme una autoritat pública (considerant 43)
- ***Dret a l'oblit*** (considerants 65 i 66): "Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un 'derecho al olvido'".

Quin és l'objecte de l'RGPD?

L'objecte últim és la protecció dels drets fonamentals de les persones físiques i tota l'afectació que **es pugui produir pel tractament de dades personals** als esmentats drets i llibertats. La garantia i protecció de les dades personals evita, així, que la resta de drets i llibertats de la persona física es vegin «tacats» o «negats» per **l'efecte irradiació de les dades personals**. La seguretat de les dades per part de l'autoritat pública o organisme és consubstancial, però instrumental, per complir aquests objectius.

L'article 1 RGPD condensa el seu objecte en els següents punts:

- Establir normes relatives a:
    - La protecció de les persones físiques pel que fa al tractament de les dades personals
    - La lliure circulació d'aquestes dades
- Protegir els drets fonamentals de les persones físiques i, en particular, el seu dret a la protecció de les dades personals

PERSONES MORTES:
També s'ha de tenir en compte que, tal com exposa el considerant 27, l'RGPD "no s'aplica a la protecció de dades personals de persones mortes", per tant els estats membres són competents per establir normes relatives al tractament de les dades personals de les mateixes. Vegeu al respecte l'article 3 ("Dades de les persones mortes") i la disposició addicional setena ("Accés a continguts de persones mortes") del PLOPD

S'aplica l'RGPD íntegrament als governs locals i a les seves entitats del sector públic?

L'RGPD és des del 25 de maig de 2018 una norma directament aplicable en la seva integritat a l'administració local i a les entitats del seu sector públic (amb alguna excepció puntual que es tractarà: DPD en determinades societats mercantils de capital públic, almenys en la formulació actual del PLOPD).

També s'han de tenir en compte, en un context globalitzat i de dades obertes, les normes que regulen les transferències de dades personals a tercers països o organismes internacionals (capítol V). Aquesta regulació no es tracta en la present guia, però ha de ser sempre i en tot cas tinguda en compte.

IDEA-FORÇA:

"Aunque pudiera parecer que las transferencias internacionales son poco habituales en el ámbito de los entes de la Administración Local, el uso cada vez más frecuente de tecnologías de la información y la comunicación o la generalización de servicios 'en nube' (cloud computing) supone que aumenten las posibilidades de que se trasfieran estos datos fuera del Espacio Económico Europeo dentro de los contratos de servicios informáticos".
(vegeu, així mateix, articles 45 i 46 que permeten fer aquestes transferències internacionals sense necessitat de sol·licitar autorització prèvia a l'autoritat de control)

Guía para la adaptación del Reglamento General de Protección de Datos, de las Administraciones Locales, FEMP, Grup de Treball per a la implantació del nou RGPD en les administracions locals.

Les administracions locals haurien d'haver adaptat els seus protocols, procediments i organització a les importants mesures que recull l'RGPD abans de la data indicada.

ÀMBITS D'AFECTACIÓ DE TRACTAMENTS EN L'ADMINISTRACIÓ LOCAL:

- Padró municipal
- Gestió de tributs
- Subvencions
- Smart Cities

Font: AEPD, «Protecció de Dades i Administració Local», 2018

El nou concepte de "protecció de dades" i altres definicions

El concepte de "dada personal" es recull en l'article 4, 1) RGPD en els termes següents:

"Datos personales": toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

Altres definicions que, per la seva incidència en l'activitat local, es recomana la consulta del seu abast en l'article 4 RGPD:

- Tractament
- Limitació del tractament
- Elaboració de perfils
- Seudonimització
- Responsable del tractament
- Encarregat del tractament
- Destinatari
- Violació de la seguretat de les dades personals
- Dades biomètriques

Dades biomètriques: "Tendrán la consideración de datos sensibles solo cuando sean utilizados para identificar unívocamente a una persona" (AEDP, *Protección de Datos y Administración Local*)

En particular, per la importància que té en el nou règim jurídic de la protecció de dades personals, és important la definició de "Consentiment de l'interessat" recollida per l'article 4, 11) RGPD:

"Consentimiento del interesado": toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

"Interessat" o "afectat"? L'AEPD recomana utilitzar l'expressió d'"afectat" i no la d'"interessat", per no incórrer en confusió amb la terminologia establerta en la Llei 39/2015, d'1 d'octubre, de procediment administratiu comú de les administracions públiques (*Protecció de Dades i Administració Local*). El PLOPD fa servir el concepte "afectat".

Quins són els principis que s'han de tenir en compte en tot tractament de dades personals?

Els principis de protecció de dades es recullen en el capítol II RGPD i alguns d'ells es desenvolupen en el PLOPD (inexactitud de les dades, deure de confidencialitat, consentiment afectat i de menors, etc.).

Els principis es poden sistematitzar partint de la regulació que recull el mateix article 5 RGPD:

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

Sens dubte, per la seva novetat o per la seva incidència en l'activitat local cal destacar, entre d'altres principis, els tres següents:

Limitació de la finalitat: Les dades personals seran recollides "con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines"

UN EXEMPLE:

Tal com recull la Guía para la adaptación al RGPD de la Administración Local (FEMP), un possible supòsit d'aplicació del principi de limitació de la finalitat de les dades seria el següent:

"¿Podría comunicarse por parte de un Ayuntamiento los datos de menores en situación de riesgo a una Mancomunidad que presta servicios sociales?"

Al marge d'altres consideracions generals que es realitzen, es conclou de la manera següent:

"En todo caso, será preciso tener especialmente en cuenta que l'RGPD regula el principio de limitación de la finalidad, es decir, que los datos no podrán ser utilizados para fines incompatibles con los fines iniciales. Por ello, la utilización de los datos para cualquier otra finalidad distinta de la relacionada con el ejercicio de las competencias en materia de atención a menores que tiene atribuida legalmente, precisaría de otra legitimación específica a la luz de las normas de protección de datos de carácter personal" (pàg. 56-57)

Minimització de les dades: "Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"

UN EXEMPLE:

Tal com recull la Guía para la adaptación al RGPD de la Administración Local (FEMP), alguns possibles supòsits d'aplicació del principi de minimització de dades serien:

- "La incorporación, tanto en la firma de los documentos electrónicos o en papel como en la marca de agua, del dato relativo al DNI del funcionario firmante, podría constituir un tratamiento excesivo y, en consecuencia, contrario al principio de minimización de datos del artículo 5 de l'RGPD" (pàg. 50)

- "Con carácter general, las grabaciones indiscriminadas de voz y de conversaciones del público en general que acceden a los edificios de un Ayuntamiento a través de sistemas de videovigilancia, no cumpliría el principio de minimización de datos, considerándose una medida intrusiva" (pàg. 52)

Limitació del termini de conservació: "Los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado".

BASE JURÍDICA

Licitud del tractament (article 6 RGPD: consultar): "El tratamiento solo será lícito si cumple (entre otras) alguna de estas condiciones:

- El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

- El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte

- **El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable de tratamiento**

- Tratamiento para otros fines distintos de aquel para el que se recogieron los datos personales (ALERTA): article 6.4 RGPD

- **El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos** conferidos al responsable del tratamiento".

IDEA-FORÇA:

El considerant 26 exposa: "los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable". Por tanto, deben seguirse fielmente en toda operación de tratamiento de datos personales que lleven a cabo el responsable o el encargado del tratamiento.

CATEGORIES DE DADES PERSONALS OBJECTE DE TRACTAMENT PER L'ADMINISTRACIÓ LOCAL:

- De caràcter identificatiu (nom, cognoms, telèfon, DNI, imatge)

- De caràcter tributari

- Acadèmics i professionals (selecció, bosses, Recursos Humans)

- Exercici de potestat sancionadora

- Categories especials de dades

- Smart cities

Vegeu: AEDP, *Protecció de Dades i Administració Local.*

El PLOPD conté algunes previsions que convé tenir presents:

- **Disposició addicional novena.** Identificació dels interessats en les notificacions per mitjà d'anuncis i publicacions d'actes administratius
- **Disposició addicional quinzena.** Disposicions específiques aplicables als tractaments dels registres de personal del sector públic

Quina és la nova configuració del "consentiment" en l'RGPD?

Ja s'ha vist la definició de consentiment de l'interessat. Quan no hi ha "base legal" o base jurídica específica, l'administració pública ha de sol·licitar inexcusablement el consentiment exprés i inequívoc de l'interessat. L'article 6 PLOPD reenvia a la regulació de l'RGPD, excepte algunes precisions (consentiment quan hi hagi pluralitat de finalitats en un tractament). Hi ha una regulació particular sobre el consentiment del nen (article 8 RGPD) o del menor d'edat (article 7 PLOPD). Particular importància té per a l'administració local que estableix l'article 6.1 c) RGPD i l'article 8 LOPD, sobre tractament de dades emparades per la Llei (base jurídica legal).

En tot cas, s'han de tenir en compte les disposicions addicionals tretzena i transitòria sisena del PLOPD, que es recullen al final d'aquest epígraf.

En aquest nou àmbit de regulació cal ressaltar el que estableix l'article 7 RGPD relatiu al que s'ha denominat Condicions per al consentiment. Vegem algunes de les més rellevants:

Condicions per al consentiment (selecció):

- Si el tractament es basa en el consentiment de l'interessat: "El responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales" (càrrega de la prova del responsable)

- Si el consentiment es produeix en un context de declaració escrita que faci referència també a unes altres qüestions el "consentimiento se prestará de tal forma que se distinga claramente de los demás asuntos de forma ineludible y de fácil acceso y utilizando un leguaje claro y sencillo".

- "El interesado tendrá derecho a retirar su consentimiento en cualquier momento (...) Será tan fácil retirar el consentimiento como darlo".

PROJECTE DE LLEI ORGÀNICA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

El PLOPD recull, així mateix, algunes disposicions que, directament o indirectament, poden afectar el consentiment.

Així, la **disposició addicional desena ("Potestat de verificació de les administracions públiques")** recull el següent:

"Cuando se formulen solicitudes por medios electrónicos en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos".

Per la seva banda, **la "disposició addicional tretzena (" Comunicacions de dades pels subjectes enumerats en l'article 77.1"),** sembla advertir un debilitament de les exigències del consentiment segons l'RGPD quan actuen entitats del sector públic en determinades circumstàncies:

"Los responsables enumerados en el artículo 77.1 de esta Ley orgánica podrán comunicar los datos de carácter personal que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos o intereses de los afectados conforme a lo establecido en el artículo 6 1 f) del Reglamento (UE) 2016/679".

I, finalment, **la disposició transitòria sisena ("Consentimientos otorgados con anterioridad a la aplicación del Reglamento (UE) 2016/679"),** exposa:

"Cuando el tratamiento se base en un consentimiento otorgado con anterioridad a la aplicación del Reglamento (UE) 2016/679, no será necesario recabar nuevamente dicho consentimiento si la forma en que se otorgó se ajusta a las condiciones del Reglamento (UE) 2016/679".

UNA POSSIBLE APLICACIÓ:

Per part d'alguna opinió doctrinal s'ha posat en relleu que l'incís segon de l'apartat 2 de l'article 28 de la Llei 39/2015, d'1 d'octubre, quedaria desplaçat per l'RGPD quan afirma que "es presumeix que la consulta o obtenció és autoritzada pels interessats, llevat que consti en el procediment la seva oposició expressa o la llei especial aplicable requereixi consentiment exprés". El problema, certament, és que en aquest cas es preveu un consentiment tàcit o presumpte que no s'adequa, en principi, a les exigències de l'RGPD.

Vegeu: Concepción Campos Acuña, "Los 7 imprescindibles en protección de datos para el ámbito local", El Consultor de los Ayuntamientos y Juzgados, gener 2018 https://bit.ly/2EftpAb

Cal considerar que si prospera l'actual redacció de la disposició adicional desena del PLOPD, les administracions públiques han de tenir la potestat de verificar en tot cas, i sense necessitat de consentiment, les dades que els usuaris manifestin en les sol·licituds mitjançant una declaració responsable. Aquest fet suposa una millora considerable en l'aplicació pràctica de la simplificació de procediments i compliment normatiu, quant a no demanar dades ni documents a la ciutadania que ja estiguin en poder d'altres administracions públiques. Una altra cosa és que, òbviament, es requereix informar degudament d'aquest fet a la ciutadania (en els termes recollits per l'RGPD). Caldrà esperar per veure com queda regulada definitivament aquesta matèria en la futura LOPD i com es cohonesten les previsions de l'RGPD amb aquesta finalitat de simplificació administrativa.

En tot cas, **la tesi de l'AEPD és que la redacció actual de l'article 28.2 de la Llei 39/2015, podria trobar fonament en l'article 6.1 i) RGPD, en concret** "quan el tractament sigui necessari per al compliment d'una missió realitzada en interès públic o en l'exercici de poders públics conferits al responsable del tractament "(Vegeu: *Protecció de Dades i Administració Local*, pàg. 13).

En el cas de la interoperabilitat dels registres electrònics de les administracions públiques, el tractament podria emparar-se en el compliment d'una obligació legal aplicable al responsable del tractament o, així mateix, que aquest tractament és necessari per a l'exercici de poders públics conferits al responsable del tractament (article 6, 1 c) o 6,1 e) RGPD)

Els tractaments de "categories especials"

En els considerants es fa alguna menció específica a la noció "dades sensibles", però l'RGPD en el seu article 9 es refereix a la noció de "categories especials de dades personals", en els termes següents:

Categories especials de dades personals:

9.1 RGPD: "Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física".

PER SABER-NE MÉS:

Pel que fa al tractament de categories especials de dades i les excepcions aplicables a l'Administració Local, vegeu: AEDP, *Protecció de Dades i Administració Local,* pàg. 14

Quins drets garanteix l'RGPD a l'"interessat" o « afectat »?

L'RGPD conté una nova regulació dels drets de les persones en matèria de protecció de dades. Els vells drets ARCO es mantenen o es modulen, però s'incorporen uns altres amb perfils nous, especialment com es veurà a continuació el dret d'informació als afectats.

Aquesta important regulació està recollida en el capítol III ("Drets de l'interessat"), articles 12 a 22. El PLOPD també preveu una regulació d'aquests drets, però excepte en aquells drets que afecten la transparència i informació a l'afectat (article 11), dret d'accés (article 13) i dret de rectificació (article 14), que completen el que preveu el Reglament, en la resta es duu a terme un simple reenviament al que estableix l'RGPD.

Per tant, tenint en compte les finalitats de l'RGPD, les administracions locals en els processos de tractament de dades han d'adoptar mesures de caràcter tècnic, organitzatiu i de seguretat encaminades a no afectar cap dels drets que s'hi recullen.

La dada sempre és de la persona, la gestió de la dada quan l'exerceix una autoritat o organisme públic és administrativa, però emmarcada en el conjunt de principis, limitacions i drets establerts per l'RGPD.

DRETS DE L'INTERESSAT O AFECTAT:

- Transparència de la informació (articles 12-13-14)
- Dret d'accés (article 14)
- Dret de rectificació (article 16)
- Dret de supressió o "dret a l'oblit" (article 17)
- Dret a la limitació del tractament (article 18)
- Dret a la portabilitat de les dades (article 20)
- Dret d'oposició i a no ser objecte de decisions individuals automatitzades (articles 21-22)

SI VOSTÈ ÉS CIUTADÀ, CONEGUI ELS SEUS NOUS DRETS EN RELACIÓ AMB LES DADES

NOUS DRETS	ARTÍCLES RGPD
Dret a rebre informació clara i comprensible	(Artícles 12-14)
Dret a solicitar accés a les dades personals que una organització té sobre vostè	(Artícle 15)
Dret a sol·licitar a un proveïdor de serveis que transmeti les seves dades personals a un altre o que li faciliti	(Artícle 20)
Dret a l'oblit	(Artícle 17)
Consentiment exprés (Ja no hi ha extenses condicions jurídiques que vostè mai es llegeix)	(Artícles 4.11 y 7)
Si les seves dades es perden o són robades: Dret a ser informat sense dilació indeguda	(Artícles 33-34)
Major protecció en línia per als menors	(Artícle 8)

[Font: Comissió Europea, gener 2018 (data protection-factsheet-citizens_es)]

IDEA-FORÇA SOBRE ELS DRETS A L'RGPD:

- **Enfortiment dels drets de les persones:** el Reglament introdueix nous requisits de transparència; drets reforçats d'informació, accés i eliminació («dret a l'oblit»); el silenci o la falta d'activitat deixaran de considerar-se com un consentiment vàlid, ja que es requereix una clara acció afirmativa per expressar aquest consentiment; i la protecció dels nens en línia.

(Font: Comunicación de la Comisión al Parlamento Europeo y al Consejo. Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018 Bruselas 20-1-2018 COM (2018) 43 final)

Quin és el nou marc normatiu de la informació i com afecta les entitats locals?

Sota l'enunciat de "Transparència i modalitats", els articles 12 a 14 de l'RGPD contenen una nova regulació de la informació i de les comunicacions que s'ha de proveir a les persones físiques quan es tractin les seves dades. Un desenvolupament d'aquestes previsions quedat recollit per l'article 11 del PLOPD.

L'RGPD preveu, així, **la transparència com a principi** (que ha de ser especialment tingut en compte per l'administració pública en l'exercici de les seves funcions de tractament de dades) **i com a dret de les persones físiques en relació amb les seves dades de caràcter personal.**

Les novetats més significatives d'aquest nou marc normatiu van encaminades a reforçar notablement l'obligació d'informació en tot procés de tractament de dades, la qual cosa obligarà les administracions locals a tenir en compte aquestes noves exigències.

Alguns trets d'aquest dret a ser informat són:

- El responsable del tractament ha de prendre les mesures oportunes per a facilitar a l'interessat tota la informació relativa al tractament, de manera concisa, transparent, intel·ligible i de fàcil accés, amb un llenguatge clar i senzill

- El responsable del tractament ha de facilitar a l'interessat l'exercici dels seus drets i, així mateix, també li proveirà la informació relativa a la seva sol·licitud en el termini d'un mes o, excepcionalment, en dos quan s'invoqui complexitat o un nombre elevat de sol·licituds. Si no dona curs a la seva sol·licitud, la informació serà realitzada sense dilació o com a màxim en un mes. Hi ha una possible pròrroga de dos mesos.

- La informació sol·licitada serà gratuïta, llevat d'excepcions taxades (article 12.5)

- Entre la informació que s'ha de facilitar quan les dades s'obtinguin de l'interessat, es troba la següent:

  - Identitat i dades de contacte del responsable
  - Les dades de contacte del delegat de protecció de dades
  - Les finalitats del tractament a què es destinen les dades personals i la base jurídica del tractament
  - El termini en el qual es conservaran les dades personals
  - L'existència del dret a sol·licitar del responsable del tractament l'accés a les dades personals, la rectificació o supressió, la limitació del tractament, l'oposició o la portabilitat de les dades.

- Quan les dades no s'hagin obtingut de l'interessat caldrà afegir a la informació anterior, "la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público".

Les autoritats de control de protecció de dades han elaborat conjuntament una Guia per al compliment del deure d'informar a l'RGPD, que es pot consultar en la seva versió en llengua catalana accedint mitjançant l'enllaç següent: http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/

PEL QUE FA AL DEURE D'INFORMACIÓ EXERCIT PER LES ADMINISTRACIONS PÚBLIQUES, QUÈ CANVIA L'RGPD?

Informació que cal facilitar actualment (LO 15/1999)	**NOU: Informació addicional que s'ha d'afegir per aplicació de l'RGPD**
L'existència del fitxer o tractament	Les dades de contacte del delegat de protecció de dades
El caràcter obligatori o no de la resposta, així com les seves conseqüències	La base jurídica o legitimatzió del tractament
La possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició	La previsió de transferències a tercers països i l'existència d'una decisió d'adequació o de garanties adequades i els mitjans per a obtenir una còpia
La identitat i les dades de contacte del responsable de tractament	El termini o els criteris de conservació de la informació
	El dret a solicitar la limitació del tractament i la portabilitat de les dades
	(*) L'article 14.2 b) no s'aplica a les autoritats i organismes públics

RECOMANACIÓ DE LES AUTORITATS DE CONTROL SOBRE LAS OBLIGACIONS D'INFORMACIÓ DE L'RGPD:

"En consecuencia, los procedimientos, modelos o formularios diseñados de conformidad con la LOPD se han de revisar y adaptar antes de la fecha de plena aplicación de l'RGPD, para incorporar allí los nuevos requisitos"

"Se recomienda revisar y aplicar esta adaptación sin que quepa esperar a la fecha de plena aplicación de l'RGPD"

INFORMACIÓ PER CAPES:

Cal delimitar el dret a la informació en una "**informació per capes**", informació bàsica (primer nivell) i una informació addicional (segon nivell):

Presentar la informació bàsica en un 1r nivell:

- de forma resumida,

- en el mateix moment i

- en el mateix mitjà de recollida

Remetre a informació addicional en un 2n nivell:

- de manera detallada,

- en un mitjà més adequat per a la seva presentació, comprensió i arxiu

RECOMANACIÓ AEPD: TRACTAMENT PER CAPES

Pel que fa al "Cumplimiento del principio de transparencia: derecho a la información en la recogida de datos personales, con la finalidad de facilitar ese cumplimiento la AEPD recomienda adoptar un modelo de información por capas o niveles. Una buena información sobre cómo llevar a cabo ese tratamiento por capas se recoge en el Cuadro de la página 28 del documento Protección de Datos y Administración Local. Vegeu-ho a la pàgina següent.

EXEMPLE TRACTAMENT PER CAPES (AEPD, *Guía de Protección de Datos y Administración Local*, abril 2018)

EPÍGRAFE	INFORMACIÓN BÁSICA (1ª Capa resumida)	INFORMACIÓN ADICIONAL (2ª Capa detallada)
Responsable del tratamiento	Identidad del responsable del tratamiento	1.- Datos de contacto 2.- Identidad/Datos contacto representante 3.- Datos contacto DPD
Finalidad del tratamiento	Descripción sencilla de los fines del tratamiento, incluso elaboración perfiles	1.- Descripción ampliada fines del tratamiento 2.- Plazos y criterios de conservación de los datos 3.- Decisiones automatizadas, perfiles y lógicas ampliadas
Legitimación del tratamiento	Base jurídica del tratamiento	1.- Detalle base jurídica, en los casos de obligación legal, interés público o interés legítimo 2.- Obligación o no de facilitar datos y consecuencias de no hacerlo
Destinatarios de cesiones o transferencias	Previsión o no de cesiones Previsión de transferencias o no a terceros países	Destinatarios o categorías de destinatarios Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
Derechos de las personas interesadas (o afectadas)	Referencia al ejercicio de derechos	1.- Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición de su tratamiento 2.- Derecho a retirar el consentimiento prestado 3.- Derecho a reclamar ante la autoridad de control
Procedencia de los datos	Fuentes de los datos cuando no proceden del interesado (o afectado)	1.- Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público. 2.- Categorías de datos que se traten

Dret d'accés

El dret d'accés de l'interessat es manifesta en el dret a obtenir del responsable del tractament confirmació sobre si s'estan tractant dades personals, així com en aquest cas el dret d'accés a les dades i a la informació recollida per l'article 15.1 RGPD.

ACLARIMENT SOBRE EL DRET D'ACCÉS RGPD:

"Debe distinguirse del derecho de acceso de los interesados a los expedientes administrativos que regula la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, así como del derecho de acceso regulado en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno" [así como del mismo derecho de acceso a la información pública regulado en la Ley 19/2014, de 29 de diciembre, del Parlamento de Cataluña, sobre transparencia, acceso a la información pública y buen gobierno"]

Guía para la adaptación del Reglamento General de Protección de Datos de las Administraciones Locales, FEMP, pàg. 24

Dret de rectificació i supressió ("Dret a l'oblit")

L'interessat té dret a demanar la **rectificació** de les dades personals inexactes o que no siguin veraces, així com al fet que es completin les dades personals que estiguin incomplets. Aquesta rectificació la durà a terme el responsable del tractament, i no podrà patir dilacions indegudes.

No hi ha novetats rellevants pel que fa a la rectificació de les dades, però sí a l'anomenat **dret a l'oblit o la supressió de dades personals**, que és, sens dubte, un dels elements nous de la regulació.

El responsable del tractament està obligat a suprimir les dades personals sempre que concorrin alguna de les circumstàncies establertes en l'article 17.1 RGPD.

En efecte, l'RGPD ha sumat el «**dret a l'oblit**» o dret de supressió als clàssics drets ARCO -accés, rectificació, cancel·lació i oposició-, la qual cosa és «un dret de cancel·lació actualitzat». Tant el considerant 65 com l'article 17 de l'RGPD exposen que els interessats tenen dret a l'oblit si la retenció de les seves dades impedeix el que disposa el mateix RGPD o la normativa de l'estat membre. Així mateix, afirma que els interessats «deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos" o si s'oposen al tractament "si los interesados han retirado su consentimiento". També indica que hauran de ser suprimides les dades personals tractades il·lícitament.

Si les dades es fan públiques, el responsable de tractament haurà d'adoptar mesures raonables per informar els responsables que estiguin tractant aquestes dades, així com per suprimir qualsevol enllaç, còpia, o rèplica dels mateixos, tenint en compte la tecnologia disponible i el cost de la seva aplicació.

Dret a la limitació del tractament

Així mateix, l'RGPD recull expressament el dret a la limitació del tractament (article 18), sempre que no concorri alguna causa legalment prevista. Aquest dret no és absolut, i es podrà dur a terme quan es doni alguna de les condicions següents:

- Es pot limitar el tractament de les dades de l'interessat quan aquest hagi impugnat la seva exactitud, durant el termini que el responsable els hagi de verificar
- Si el tractament és il·lícit, l'interessat podrà demanar la limitació de l'ús de les dades en comptes de la seva supressió
- Quan el responsable ja no necessiti fer ús d'aquestes dades, però l'interessat les necessiti per a interposar o defensar reclamacions
- Quan l'interessat s'hagi oposat al tractament de les seves dades per motius relacionats amb la seva situació particular, mentre es verifica si els motius s'han de tenir en compte

Dret a la portabilitat de les dades

El dret a la **portabilitat de les dades** suposa el "derecho del interesado a recibir su información en un formato estructurado y de uso común, para su trasmisión a otro responsable o, incluso la obligación del anterior responsable de hacerlo directamente", això últim serà possible quan sigui tècnicament viable.

- **Major control sobre les dades personals per als particulars**. El Reglament estableix **un nou dret a la portabilitat de les dades** que permet als ciutadans sol·licitar que una empresa o organització li retorni les dades personals que li va facilitar per consentiment o contracte; també permetrà que aquestes dades personals es transmetin directament a una altra empresa o organització, quan sigui tècnicament possible.

(Font: Comunicación de la Comisión al Parlamento Europeo y al Consejo. Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018 Bruselas 20-1-2018 COM (2018) 43 final)

Esquema d'Idees-Força:

- L'article 20 RGPD crea un nou dret a la portabilitat de les dades estretament relacionat amb el dret d'accés encara que diferent d'aquest últim en molts aspectes
- El propòsit d'aquest nou dret és capacitar l'interessat i donar-li més control sobre les dades personals que li concerneixen
- El dret a la portabilitat de les dades és també una eina important que donarà suport a la lliure circulació de dades personals a la UE i facilitarà el canvi entre diferents proveïdors de serveis i, per tant, la difusió de nous serveis en el context de l'estratègia per al mercat digital
- Una pràctica recomanable és que els responsables del tractament comencin a desenvolupar els mitjans que contribueixin a respondre a les sol·licituds de portabilitat

PER SABER-NE MÉS:

Grup de Treball sobre Protecció de Dades de l'Article 29: *Directrices sobre el derecho a la portabilidad de los datos*, 16/ES, WP 242 rev. 01 (Adoptades el 13 de desembre de 2016. Revisades per última vegada i adoptades el 5 d'abril de 2017)

http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/altres_documents_del_grup_de_larticle_29/

Dret d'oposició i decisions individuals automatitzades

L'interessat podrà, sempre que no concorri alguna de les excepcions previstes en el Reglament, **oposar-se** a què les seves dades siguin objecte de tractament. Aquesta oposició es podrà presentar en qualsevol moment, i es podrà basar en motius relacionats amb la situació particular de l'interessat. Si es presenta l'oposició, el responsable del tractament ha de deixar de tractar les dades personals.

Limitacions

Els drets esmentats no són absoluts, sinó que es poden trobar limitats per diversos factors.

És el responsable o l'encarregat del tractament, **a través de mesures legislatives**, el que pot limitar aquests drets, sempre que les mesures adoptades siguin necessàries i proporcionades i respecti el que preveu la normativa en aquest supòsit, així mateix la limitació haurà de respectar sempre en les qüestions essencials els drets i llibertats fonamentals.

L'article 23 de l'RGPD disposa els casos en què s'accepta la limitació dels drets de l'interessat, atenent, sempre, a la necessitat de salvaguardar, entre d'altres, la defensa, la prevenció, investigació o enjudiciament d'infraccions penals, la seguretat pública, la protecció de l'interessat o dels drets i llibertats dels altres.

3. NOU SISTEMA INSTITUCIONAL I DE GESTIÓ DE PROTECCIÓ DE DADES EN L'ADMINISTRACIÓ PÚBLICA

Introducció

El nou model de Protecció de Dades que preveu l'RGPD s'assenta sobre la **responsabilitat proactiva**, la qual cosa té especials conseqüències a l'hora d'articular el sistema institucional i de gestió de protecció de dades en les administracions locals.

Per tant, es posa l'accent en l'anàlisi de riscos i en l'avaluació d'impacte que comporta determinats tractaments de dades personals; és a dir, **el focus se situa en l'anticipació i en la prevenció, una mena de garantia i aplicació de la política de compliment (compliance) també en les organitzacions públiques.**

No cal dir que **aquest enfocament de riscos i preventiu implica un canvi de cultura organitzativa frontal pel que fa al tractament de dades.** Almenys imposa una forma diferent de treballar en tots els processos, procediments i projectes que impliquin tractar dades de forma massiva, que comportin alt risc i aquells altres que s'enquadren en "categories especials" (dades sensibles).

I és aquí on es troben els principals problemes per transitar correctament d'un model de protecció de dades "reactiu" a un altre "proactiu". La formació es torna ineludible i les polítiques de sensibilització que han de dur a terme les autoritats de control (apdCAT/AEPD/AVPD), juntament amb les administracions públiques, són una eina o palanca de canvi o transformació imprescindible per anar introduint de mica en mica **la nova cultura de gestió en la protecció de dades personals.**

El trànsit serà lent, també en el sector públic. S'ha començat tard i caldrà ajustar gradualment els diferents elements d'aquesta nova arquitectura institucional i de gestió que haurà de funcionar en un termini raonable de forma harmònica, sobretot si es vol que les dades personals i els drets fonamentals de les persones físiques no pateixin menyscabament.

De fet, aquest nou sistema de gestió hauria d'estar ja llest amb anterioritat al 25 de maig de 2018, però la seva posada en marxa en el sector públic es dilatarà en el temps, almenys en alguns casos. En qualsevol cas, no hi ha excusa, ja que l'RGPD es va aprovar amb un llarg període que diferia la seva aplicabilitat precisament per garantir la seva efectivitat i dur a terme el procés d'adaptació.

I, per articular raonablement, les diferents peces que graviten al voltant de la construcció d'aquest nou model institucional i de gestió de la protecció de dades personals en el sector públic, s'han de tenir presents, a banda dels principis i drets abans recollits, un sèrie d'elements organitzatius i institucionals que tendeixen a configurar un nou **sistema de gestió de la protecció de dades en el sector públic que es configura dels elements bàsics següents:**

Elements bàsics del sistema de gestión de protecció de dades	***Ubicació sistemàtica en l'RGPD***
Responsables/ Encarregats del tractament	Capítol IV RGPD (articles 24-29)
Registre de les activitats de tractament	Article 30 RGPD
Seguretat de les dades personals	Articles 32-34 RGPD
Anàlisi de riscos	Procés previ, si escau, a l'avaluació d'impacte
Avaluació d'impacte relativa a la protecció de dades	Articles 35-36
Delegat de protecció de dades	Articles 37-39
Codis de conducta	Articles 40-41
Mecanismes de certificació	Articles 42-43
Autoritats de control (AEPD/APDCAT)	Articles 51-59 (especialment) Títol VII PLOPD
Règim de sancions	Capítol VIII RGPD Títol IX PLOPD

L'objecte, per tant, d'aquesta tercera part de la Guia no és un altre sinó analitzar breument i de forma descriptiva aquests elements que configuren l'arquitectura bàsica del sistema institucional i de gestió de la protecció de dades en les organitzacions públiques, amb la finalitat que aquesta anàlisi serveixi com a mitjà per activar la posada en marxa de totes aquestes peces d'un complex engranatge al més aviat posible per part de les administracions locals i el de les entitats del sector públic institucional.

Responsables de tractament i encarregats de tractament: les seves peculiaritats aplicatives en l'àmbit del govern local

Responsable de tractament

El considerant 78 RGPD comença de la manera següent: "La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento".

La posada en marxa d'aquestes mesures tècniques i organitzatives apropiades és una responsabilitat d'una figura clau en el model de protecció de dades, també en el sector públic: el responsable del tractament. Al costat d'aquesta figura també es troba una altra que és la de l'"encarregat del tractament", totes dues han d'estar en condicions de complir les seves obligacions en matèria de protecció de dades. I, a més, implantar els principis de protecció de dades des del disseny i per defecte, tal com es veurà.

Dos considerants són importants en aquesta matèria. I convé reproduir-los per poder extreure les seves conseqüències efectives:

CONSIDERANT 79:

"***La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento***, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, ***requieren una atribución clara de las responsabilidades en virtud del presente Reglamento***, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable".

CONSIDERANT 81:

"**Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías**, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable. **El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable**, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado (…) Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos."

La figura del responsable de tractament ve definida en l'article 4.7 RGPD en els termes següents:

"'**RESPONSABLE DE TRATAMIENTO**' O '**RESPONSABLE**': La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros determine los fines y medios del tratamiento (…)"

La regulació específica de la figura del responsable de tractament es troba en els articles 24 a 27 RGPD, si bé el Reglament està ple de referències permanents a aquesta figura, que es transforma així en peça clau per garantir el perfecte compliment de les obligacions derivades de la norma europea o del dret intern dels estats membres, així com en garant últim perquè s'adoptin les mesures tècniques i organitzatives apropiades per a la seva adequació a aquesta normativa.

Aquesta idea es reflecteix perfectament en l'article 24 RGPD, l'apartat 1 exposa, per exemple, el següent:

"Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa a probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario."

Tal com expressa l'article 24.3 RGPD l'adhesió a codis de conducta o mecanismes de certificació "podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento".

L'article 25 RGPD, per la seva banda, recull una de les idees substantives del nou model centrat específicament en la gestió de riscos, la qual cosa es tractarà en l'epígraf d'aquesta guia relatiu a l'anàlisi de riscos, però convé reproduir, per la seva importància implícita, els apartats 1 i 2 de l'esmentat precepte. Com es pot advertir la protecció de dades des del disseny i per defecte és responsabilitat exclusiva del mateix responsable del tractament, que haurà d'aplicar les mesures tècniques i organitzatives apropiades tenint en compte el que estableix el primer incís d'aquest mateix precepte.

ARTICLE 25.1 Y 2 RGPD: PROTECCIÓ DE DADES DES DEL DISSENY I PER DEFECTE

1. "Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento***, medidas técnicas y organizativas apropiadas***, como la seudonimización, concebidas ***para*** aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y ***proteger los derechos de los interesados".***

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".

L'article 26 regula la figura del corresponsable i el règim aplicable.

El PLOPD estableix una minuciosa regulació en el títol V del responsable i encarregat del tractament. Sense perjudici de com quedi finalment aquesta regulació en el text que definitivament s'aprovi, alguns dels punts que es tracten en relació amb el paper del responsable són els següents:

- Per tal de concretar les mesures tècniques i organitzatives que els responsables i encarregats han d'adoptar, es determinen una sèrie de supòsits en els quals es podrien produir "més riscos", la qual cosa pot ajudar a definir en quins casos es poden adoptar aquestes mesures (article 28.2 PLOPD)

- L'article 31 PLOPD regula el registre d'activitats de tractament i, entre altres coses, la necessitat de comunicar per part del responsable o de l'encarregat del tractament al delegat de protecció de dades "cualquier adición, modificación o exclusión del contenido del registro"

- També en aquest mateix article 31.2 PLOPD s'estableix l'obligació que les administracions locals i les seves entitats del sector públic (recollides en l'àmbit d'aplicació de l'article 77.1 PLOPD) facin públic un inventari d'activitats de tractament

- S'estableix l'obligació del responsable del tractament de "bloquear los datos cuando proceda a su rectificación o supresión", la determinació de a disposició de quina autoritat queden aquestes dades, així com que «los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior» (article 32, 1 a 3). L'apartat 4 preveu un règim d'excepcions que poden definir-se per les autoritats de control en els termes que s'hi preveuen.

En l'àmbit local de govern la figura del responsable de tractament serà l'alcalde o alcaldessa, llevat que aquesta atribució hagi pogut ser delegada en un membre del seu equip de Govern o, així mateix, en la persona titular d'un òrgan directiu en els municipis de gran població. Al municipi de règim especial de Barcelona, aquestes responsabilitats podrien ser delegades en l'estructura gerencial o directiva.

UNA PROPOSTA:

En tot cas, atenent la importància estratègica o nuclear que té la figura del responsable en l'aplicació efectiva del nou model de gestió de l'RGPD, caldria plantejar-se l'oportunitat d'elaborar, almenys en determinades entitats locals de certes dimensions, un reglament municipal o provincial de protecció de dades que, amb un evident caràcter organitzatiu, determinés no només el paper del responsable o responsables en l'estructura municipal en matèria de protecció de dades, sinó també les seves relacions amb la figura de l'encarregat o encarregats de tractament, així com en relació amb el delegat de protecció de dades (i la definició concreta d'aquesta figura en l'organització), podent igualment regular altres aspectes específics de la matèria (seguretat, registre d'activitats, anàlisi de riscos, avaluació d'impacte, etc.).

També caldria plantejar-se si tota aquesta informació i l'organització no es poden seguir reflectint en el document de seguretat, atès que es podria considerar vigent en tant que no contradiu el que preveu l'RGPD. En qualsevol cas, el canvi de paradigma és tan profund (almenys en les seves finalitats i arquitectura institucional) que potser requereixi plantejar-se (ni que sigui com a mera hipòtesi) un reflex normatiu, com abans s'indicava.

PER SABER-NE MÉS

Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento, AEPC, apdCAT, AVPD, 2018.

http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf

Encarregat de protecció de dades

Ja s'ha vist com el considerant 97 delimita a trets generals quin és el paper i perfil que ha de tenir aquesta figura. La seva regulació en l'RGPD es troba recollida en els articles 28 i 29, principalment en el primer que resulta fonamental per concretar els criteris generals exposats en el considerant 97 sobre quin és el règim aplicable a la figura de l'encarregat de tractament.

Donada la finalitat de l'RGPD de protecció de les dades de caràcter personal i, concretament, dels drets fonamentals de les persones físiques que es puguin veure afectades per aquestes dades, la norma europea introdueix algunes novetats importants en la regulació de l'encarregat del tractament, amb l'objectiu d'apuntalar el compliment estricte del reglament, ja que en les administracions locals les dades en unes ocasions seran tractades per encarregats "interns", però en unes altres serán tractades per encarregats "externs", mitjançant procediments de contractació pública, encàrrecs de gestió, convenis o altres instruments jurídics.

De ahí que la regulación de esta figura se prevea con cierto detalle. Y de ahí también cómo las autoridades de control (AEPD/apdCAT/AVPD) han elaborado, según se verá de inmediato, un documento de notable interés sobre el encargado del tratamiento y, asimismo, sobre el papel del responsable de tratamiento en relación con aquel.

Per aquest motiu la regulació d'aquesta figura es preveu amb cert detall. I d'aquí també com les autoritats de control (AEPD/apdCAT/AVPD) han elaborat, segons es veurà immediatament, un document de notable interès sobre l'encarregat del tractament i, així mateix, sobre el paper del responsable de tractament en relació amb el primer.

PER SABER-NE MÉS:

"Directrices para la elaboración de contratos entre responsables y encargados de tratamiento".

La versió en català d'aquest document ha estat difosa per apdCAT amb el títol Guia sobre l'encarregat del tractament al RGPD; http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/guia_sobre_lencarregat_del_tractament_al_rgpd/

La regulació substantiva d'aquesta figura es porta a terme en l'article 28 RGPD, del que es poden destacar els aspectes següents:

- L'apartat 1 exposa el següent: "Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, éste **elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas**, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado."

- L'apartat 2 regula que l'encarregat del tractament no podrà recórrer a un altre encarregat sense l'autorització prèvia per escrit, específica o general, del responsable. Haurà d'informar de qualsevol canvi

- **El tractament per l'encarregat es regirà per un contracte o acte jurídic**, que haurà d'estipular, en particular, una sèrie d'exigències que es detallen en l'article 28.3 RGPD

- Quan un encarregat recorri a un altre per dur a terme determinades activitats de tractament per compte del responsable, se li han d'imposar, també per contracte o acte jurídic, les mateixes obligacions de protecció de dades estipulades en el contracte o acte jurídic existents entre el responsable i l'encarregat principal (article 28.4)

- L'adhesió a codis de conducta o mecanismes de

certificació podrà ser utilitzada com a element per demostrar que es compleixen les garanties establertes en aquest article 28.1 a 4.

- Es preveu una referència a les clàusules contractuals tipus i a la facultat d'adoptar-les per la Comissió o per l'autoritat de control

- Es conté així mateix l'exigència per la qual el contracte o un altre acte jurídic sigui sempre per escrit (format electrònic, actualment)

- I, finalment, s'incorpora una important clàusula de desplaçament de la responsabilitat en determinats supòsits (article 28.10)

El PLOPD conté en el seu article 33 una regulació de la figura de l'encarregat del tractament, les notes més rellevants, sense perjudici de com quedi finalment en el text de la Llei orgànica que s'aprovi, són les següents:

- L'accés per part d'un encarregat de tractament a les dades personals que siguin necessàries per a la prestació d'un servei al responsable no es considera comunicació de dades, si es compleix el que estableix la normativa d'aplicació.

- Tindrà la consideració de responsable del tractament i no la d'encarregat qui en el seu propi nom i sense que consti que actua per compte d'un altre, estableixi relacions amb els afectats tot i que hi hagi un contracte o acte jurídic amb el contingut fixat per l'article 28.3 RGPD. S'exceptuen d'aquesta regla els encàrrecs efectuats en el marc de la legislació de contractació del sector públic.

- També es considera responsable del tractament qui figurant com a encarregat utilitzés les dades per a les seves pròpies finalitats

- El responsable del tractament ha de determinar si, quan finalitzi la prestació dels serveis de l'encarregat, les dades de caràcter personal han de ser destruïdes, retornades al responsable o lliurades, si escau, a un nou encarregat. S'estableix alguna excepció

- L'encarregat del tractament podrà conservar, degudament bloquejades, les dades quan puguin derivar responsabilitats de la seva relació amb el responsable del tractament

- **En l'àmbit del sector públic podran atribuir-se les competències pròpies d'un encarregat del tractament** a un determinat òrgan de l'Administració General de l'Estat, l'Administració de les comunitats autònomes, les entitats que integren l'administració local o als organismes vinculats o dependents de les mateixes mitjançant l'adopció d'una norma reguladora d'aquestes competències, que haurà d'incorporar el contingut exigit per l'article 28.3 del Reglament (UE) 2016/679.

DISPOSICIÓ TRANSITÒRIA CINQUENA PLOPD. CONTRACTES D'ENCARREGATS DEL TRACTAMENT

"Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y, en caso de haberse pactado de forma indefinida, hasta transcurridos cuatro años desde la citada fecha.

En caso de que los contratos previesen su prórroga al término de su vencimiento, ya fuera por mutuo acuerdo entre las partes o en ausencia de denuncia por cualquiera de ellas, deberá producirse su adaptación con anterioridad al momento en que estuviera prevista dicha prórroga".

I, finalment per tenir una idea més general del paper i de les novetats que implica la figura de l'encarregat del tractament, així com de les seves relacions amb el responsable del tractament, s'ha de consultar l'important document de Directrius per a l'elaboració de contractes entre responsables i encarregats del tractament, editat en català per apdCAT amb el títol ja indicat, que és el que s'utilitzarà com a referència en aquest text.

IDEES-FORGA de la *"Guia sobre l'encarregat del tractament al RGPD"*; http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/guia_sobre_lencarregat_del_tractament_al_rgpd/

QUÈ ÈS UN ENCARREGAT DEL TRACTAMENT I QUINA ÉS LA SEVA FUNCIÓ PRINCIPAL:

- L'encarregat del tractament és la persona física o jurídica, autoritat pública, servei o organisme que presta al responsable un servei que comporta el tractament de dades personals per compte d'aquest.
- Tot i que la definició pot semblar clara, a la pràctica es donen multitud de situacions en què pot ser difícil delimitar quan ens trobem davant d'un encarregat i quan davant d'un responsable del tractament. Per facilitar aquesta distinció, hem de tenir en compte que correspon al responsable decidir sobre la finalitat i els usos de la informació, mentre que l'encarregat del tractament ha de complir les instruccions de qui li encomana un determinat servei, en relació amb el tractament de les dades personals a les quals té accés com a conseqüència de la prestació d'aquest servei.

QUIN NIVELL DE DECISIÓ POT ASSUMIR UN ENCARREGAT DEL TRACTAMENT?

- L'encarregat del tractament pot adoptar qualsevol decisió organitzativa i operacional necessària per prestar el servei que té contractat. En cap cas pot variar les finalitats i els usos de les dades, ni pot utilitzar-les per a les seves pròpies finalitats.

- Les decisions que adopta han de respectar les instruccions del responsable del tractament.

EL RESPONSABLE DEL TRACTAMENT POT TRIAR QUALSEVOL ENCARREGAT DEL TRACTAMENT?

- El responsable del tractament ha de triar un encarregat del tractament que ofereixi garanties suficients respecte de la implantació i el manteniment de les mesures tècniques i organitzatives apropiades, d'acord amb el que estableix l'RGPD, i que garanteixi la protecció dels drets de les persones afectades. Per tant, hi ha un deure de diligència a l'hora d'escollir l'encarregat.

COM S'HAN DE REGULAR LES RELACIONS ENTRE EL RESPONSABLE I L'ENCARREGAT DEL TRACTAMENT?

- La regulació de la relació entre el responsable i l'encarregat del tractament s'ha d'establir a través d'un contracte o d'un acte jurídic similar que els vinculi. El contracte o l'acte jurídic ha de constar per escrit, inclòs en format electrònic.
- La possibilitat de regular aquesta relació a través d'un acte jurídic unilateral del responsable del tractament és una de les novetats que preveu l'RGPD. En qualsevol cas, ha de ser un acte jurídic que estableixi i defineixi la posició de l'encarregat del tractament, sempre que aquest acte vinculi jurídicament l'encarregat del tractament. Aquest seria el cas, per exemple, d'una resolució administrativa que consti notificada a l'encarregat del tractament.

QUI ÉS RESPONSABLE DELS TRACTAMENTES DUTS A TERME PER L'ENCARREGAT?

- El responsable del tractament no perd aquesta consideració en cap cas. Per tant, continua sent responsable que les dades personals es tractin correctament i de la garantia dels drets de les persones afectades. El responsable té una obligació d'especial diligència en l'elecció i la supervisió de l'encarregat.

SI S'EXTERNALITZEN LES FUNCIONS DEL DELEGAT DE PROTECCIÓ DE DADES A UN TERCER, AQUEST TÉ LA CONSIDERACIÓ D'ENCARREGAT DEL TRACTAMENT?

- Sí, l'RGPD preveu que el delegat de protecció de dades ha de poder accedir a les dades que es tractin. Per tant, s'haurà de formalitzar un encàrrec del tractament.

QUIN ÉS EL CONTINGUT MÍNIM D'UN ACORD O ACTE D'ENCÀRREC DEL TRACTAMENT? (VEGEU LA DESCRIPCIÓ DE CADA PUNT A LA GUIA: pàg. 4)

- Les instruccions del responsable del tractament
- El deure de confidencialitat
- Les mesures de seguretat
- El règim de la subcontractació
- El drets dels interessats
- Col·laboració en el compliment de les obligacions del responsable
- El destí de les dades al finalitzar la prestació
- La col·laboració per demostrar el compliment

ENCARREGAT DE TRACTAMENT: EXEMPLES QUAN UN AJUNTAMENT ENCARREGA A UN TERCER EL TRACTAMENT DE DADES.

- Elaboració de nòmines de personal
- Destrucció de documentació
- Control de càmeres de videovigilància
- Gestió de cobrament d'impostos
- Manteniment d'equips informàtics
- Font: *AEPD, Protecció de Dades i Administració Local*

Registre de les activitats de tractament

Es tracta, sens dubte, d'una de les novetats més significatives de l'RGPD, que es vincula directament amb la filosofia que impregna el nou model de gestió de dades personals.

La creació o manteniment d'un registre d'activitats de tractament és una obligació que han de complir necessàriament els responsables del tractament (o els seus representants) i els encarregats del tractament (o els seus representants). I substitueix l'antiga obligació de notificar els fitxers i tractaments a les autoritats de control (AEPD, adpCAT o AVPD). No és un registre de fitxers, sinó de tractaments.

EINES. COM IMPLANTAR EL REGISTRE D'ACTIVITATS: Un bon model de registre d'activitats de tractament, a partir del "cicle de vida de les dades", es pot trobar a: *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*, pàg. 36-39

http://www.agdp.es/portalwebAGPD/canaldocumentacion/publicaciones/index-idesidphp.php

El marc regulatori ve establert per l'article 30 RGPD. Tot i que cal tenir en compte el que estableix la futura LOPD (article 31 PLOPD).

Les administracions públiques i les seves entitats del sector públic institucional (a excepció de les societats mercantils públiques) "harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos" (article 31.2 PLOPD).

Cal tenir en compte que aquests registres d'activitats de tractament del responsable o de l'encarregat tenen una intensitat diferent quant al seu contingut, tal com estableixen els apartats 1 (responsable) o 2 (encarregat) de l'article 30 RGPD:

Responsables de tractament	***Encarregats de tractament***
Nom i dades de contacte del responsable o del seu representant	Nom i dades de contacte de l'encarregat o del seu representant
Nom i dades de contacte del DPD	Nom i dades de contacte del DPD
Finalitats del tractament	Categories de tractaments
Categories interessats i de dades personals	
Categories destinataris comunicacions, inclosos destinataris tercers països	
Transferències internacionals tercer país	Transferències internacionals tercer país
Terminis previstos supressió categories dades	
Mesures tècniques i organitzatives de seguretat: descripció general	Mesures tècniques i organitzatives de seguretat: descripció general

L'article 30.5 de l'RGPD exposa el següent:

> "Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10".

No obstant això, aquest precepte s'ha d'interpretar d'acord amb el que estableix el considerant 13 "in fine". La seva aplicabilitat com a excepció a les administracions locals s'ha d'emmarcar en aquestes exigències. Per les dades que es tracten en l'àmbit local, almenys en alguns casos, l'excepció entesa com a inaplicació sembla que no funcionaria en aquest cas.

REGISTRE D'ACTIVITATS DE TRACTAMENT ADMINISTRACIÓ LOCAL: ALGUNS EXEMPLES.

- Impost vehicles: "Por ejemplo, si los datos que se utilizan para el cobro del impuesto de vehículos se usan para informar sobre una campaña informativa sobre contaminación producida por los citados vehículos, existirán dos tratamientos de esos datos: uno respecto al cobro del impuesto y otro referente a la citada campaña" (pàg. 15-16)

- Registre d'activitats del Padró Municipal i de Seguretat, veure: pàg. 17-18

Font: AEPD, Protección de Datos y Administración Local

Seguretat de les dades personals

En l'RGPD la seguretat es vincula estretament amb la protecció de dades personals i amb la salvaguarda dels drets i llibertats de les persones físiques. Aquest és un enfocament de seguretat diferent, ja que tendeix a formar part d'aquest sistema de gestió de dades personals que ha d'activar totes les organitzacions públiques.

Les novetats que introdueix l'RGPD en aquest àmbit també són importants, sobretot per la naturalesa proactiva dels tractaments i la necessitat de tenir l'enfocament de riscos estretament vinculat amb els sistemes de seguretat. Es tracta d'imprimir un concepte de seguretat «dinàmic» o «instantani», que depèn del responsable del tractament.

El marc regulatori és molt precís: articles 32 i 33 de l'RGPD. Vegeu també la disposició addicional primera del PLOPD. En aquesta última referència s'ubicarà una modificació de l'Esquema Nacional de Seguretat per adaptar-lo a les exigències de l'RGPD, que implicarà la modificació o adaptació del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica.

Disposició addicional primera PLOPD:

"El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos de carácter personal para evitar su pérdida, alteración o acceso no autorizado, adaptando criterios de determinación del riesgo en el tratamiento de los datos en el artículo 32 del Reglamento (UE) 2016/679"

En funció d'una sèrie de variables enunciades a l'article 32.1 RGPD, "el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo", que inclou, entre d'altres qüestions:

- Seudonimització i codificació de dades personals
- Garantia de confidencialitat, integritat, disponibilitat i resiliència dels sistemes
- Capacitat de restaurar la disponibilitat i accés ràpidament en casos d'incidents
- Verificació, avaluació i valoració amb caràcter regular de l'eficàcia de les mesures tècniques i organitzatives (*) (**)

(*) Quan es valori l'adequació del nivell de seguretat, es tindran en compte els riscos (qüestió que es tracta en el següent epígraf).

(**) L'adhesió a codis de conducta i mecanismes de certificació poden servir com a mitjans de compliment dels requisits establerts

IMPORTANT PER A L'ADMINISTRACIÓ PÚBLICA I ENTITATS VINCULADES, AIXÍ COM PER ALS EMPLEATS PÚBLICS:

"El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable (...)" (Artículo 32.4 RGPD).

IDEES-FORÇA SOBRE MESURES DE SEGURETAT SEGONS AEPD:

- "El RGPD no establece medidas de seguridad estáticas, por lo que corresponderá al responsable determinar aquellas medidas de seguridad que sean necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales" (p. 20).

- "En ningún caso el RGPD se debe entender como la eliminación automática de tales medidas de seguridad ya existentes" (p. 20).

- "La seudonimización contribuye a reducir riesgos"

AEPD, *Protección de Datos y Administración Local*

***DATA BREACH:* VIOLACIONS DEL SISTEMA DE SEGURETAT**

Es tracta també d'una important novetat de l'RGPD que es regula en els articles 33 i 34, oferint un doble règim jurídic de notificació o comunicació immediata ("sense dilació indeguda") per part del responsable del tractament a l'autoritat de control i als interessats, respectivament, en els casos de violació de sistemes de seguretat que comportin pèrdua, alteració o destrucció de dades.

Hi ha, per tant, una obligació institucional doble i es troba darrere d'aquesta regulació un dret de la persona física a ser informada de les violacions del sistema de seguretat que afecten les seves dades personals. L'encarregat ho ha de posar immediatament en coneixement del responsable.

RÈGIM DE NOTIFICACIONS I COMUNICACIONS:

A l'autoritat de control. Requisits:

- Com a molt tard 72 hores després que s'hagi tingut constància de la violació

- No és necessària quan sigui improbable un risc per als drets i llibertats de la persona

- La notificació ha de recollir una sèrie d'exigències que estableix l'article 33.3 RGPD

- L'autoritat de control verifica el compliment del que preveu l'article 33 RGPD

Als interessats. Requisits:

- Es comunica la violació de les dades personals "quan sigui probable que comporti un alt risc per als drets i llibertats"

- La comunicació descriurà en un llenguatge clar i senzill la naturalesa de la violació de la seguretat, així com haurà de complir determinades exigències (article 34.2 RGPD)

- Supòsits en què no és necessària (article 34.3 RGPD)

- L'autoritat de control pot exigir al responsable de tractament que porti a terme aquesta comunicació quan no ho hagi fet

PER SABER-NE MÉS:

ARTICLE 29 DATA PROTECTION WORKING PARTY 17/EN, WP 250

Guidelines on Personal data breach notification under Regulation 2016/679

Adopted on 3 October 2017

RECOMANACIONS AEPD SOBRE FALLADES DE SEGURETAT:

- "Los entes de la Administración Local pueden elaborar un Plan de Contingencias con la finalidad de mitigar los daños cuando se produzca una quiebra de seguridad"

- "También deben mantener un registro de incidentes de seguridad" (p. 22)

AEDP, *Protección de Datos y Administración Local*

Anàlisi de riscos

L'enfocament predominantment "proactiu" del sistema de gestió de dades personals que es deriva de l'RGPD imposa al responsable i a l'encarregat del tractament l'exigència de **dur a terme amb caràcter previ una anàlisi de riscos**, per descartar com a mínim que es pugui requerir la necessitat de fer una "avaluació d'impacte relativa a la protecció de dades" que s'analitza en el següent epígraf d'aquesta Guia.

Aquesta qüestió està entrellaçada amb el sistema de seguretat que s'implanti, ja que **l'anàlisi de riscos ha de formar part de la mateixa avaluació del nivell de seguretat.**

I això ho posa en relleu l'article 32.2 RGPD de forma diàfana:

> "Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de protección de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos".

L'anàlisi de riscos es troba imbricada amb la seguretat i també amb la prevenció o anticipació, formant part "existencial" per tant del nou sistema de gestió de dades personals també en el sector públic.

Però ara ens interessa l'anàlisi de risc com a fase prèvia a l'avaluació. I, per aquest motiu, cal fer referència a un document que va elaborar en el seu moment l'AEPD sobre aquesta qüestió.

PER SABER-NE MÉS I COMPRENDRE MILLOR QUÈ ÉS UNA ANÀLISI DE RISCOS:

Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD (GARTDP)

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

El model de l'RGPD basat en un enfocament de riscos es desplega amb un caràcter preventiu amb una finalitat molt precisa: garantir els drets i llibertats dels interessats des de la definició d'una activitat de tractament.

PROTECCIÓ DE DADES PER DISSENY I PER DEFECTE:

L'article 25 RGPD, tal com s'ha dit, preveu una important regulació de la "Protecció de dades des del disseny i per defecte". I pren com a referència dues dimensions:

- ***Privacy by design. Garantir la protecció de la privacitat des de l'inici o disseny*** (les dades han de protegir-se quan es dissenyi un procés nou): Article 25.1 RGPD ("(…) el responsable del tratamiento aplicará tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas (…) para aplicar de forma efectiva los principios de protección de datos".

- ***Privacy by default. Garantir la protecció de la privacitat en tot moment o per defecte*** (les dades han d'estar sempre protegides per defecte). Article 25.2 RGPD: "El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento".

LÍNIES FORÇA DE LA GARTDP (AEPD) SOBRE ANÀLISI DE RISCOS:

- **FINALITAT:** el disseny adequat de les activitats de tractament és un aspecte clau per poder garantir els drets i llibertats dels interessats.

- **QUAN:** la fase de disseny d'un tractament defineix el flux de les dades personals i és el moment idoni per definir les mesures de control i seguretat per garantir els drets i llibertats.

- **QUÈ ÉS LA GESTIÓ DE RISCOS**: "Es el conjunto de actividades y tareas que permiten controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como las medidas para su reducción o mitigación".

- **QUINES SÓN LES ETAPES DE LA GESTIÓ DE RISCOS:** és un sistema de monitorització contínua que es pot dividir en tres etapes:
  - IDENTIFICAR les amenaces
  - AVALUAR els riscos
  - TRACTAR els riscos

- **QUÈ ÉS UNA AMENAÇA:** "Es cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos de carácter personal se realiza un tratamiento".

- **QUÈ ÉS UN RISC:** "Un riesgo se puede definir como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas".

- **TRACTAR ELS RISCOS:** "El objetivo de tratar los riesgos es disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto de que estos se materialicen.

- **DEFINICIÓ DE L'ACTIVITAT:** És el pas que requereix tenir clares quines són les finalitats del tractament, així com definir adequadament les activitats de tractament, documentant les anàlisis i deixant constància de la traçabilitat d'aquestes. S'han de tenir sempre presents en aquest tipus d'operacions els principis de l'article 5 RGPD.

IDEA-FORÇA: L'RGPD busca aprofitar els avantatges que ofereix la gestió de riscos introduint una nova visió on el ***focus d'atenció no se centra en les amenaces a la seguretat de l'organització, sinó que centra la seva atenció en les amenaces sobre els drets i llibertats dels interessats*** (és a dir, ciutadans, clients, usuaris serveis, etc.). Per tant, l'avaluació dels riscos ha de ser el resultat d'una reflexió sobre les implicacions que els tractaments de dades de caràcter personal tenen en relació amb els «interessats»

PER SABER-NE MÉS I PER APLICAR MILLOR LA GESTIÓ D'ANÀLISI DE RISCOS: És imprescindible consultar la Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales sujetos al RGPD elaborada per la AEPD

Per tal de determinar si un tractament comporta escàs risc, l'AEPD ha elaborat l'eina Facilita destinada a aquelles organitzacions i processos que impliquen escàs nivell de risc en el tractament de les dades personals, partint de la premissa que tot tractament comporta un determinat nivell de risc.

https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/herramientas_ayuda/index-ides-idphp.php

Avaluació d'impacte sobre la protecció de dades

Convé tenir clar des de l'inici que una avaluació d'impacte sobre la protecció de dades (AIPD) no es requereix sempre.

Per això és important dur a terme amb caràcter previ aquesta anàlisi de riscos (encara que en alguns casos, com es veurà, no és necessària aquesta fase si la l'AIPD és obligatòria).

L'anàlisi de riscos pot conduir perfectament al fet que no hi ha cap risc en el tractament o els riscos que comporta són d'ordre menor (fàcilment controlables), i adoptar les mesures tècniques i organitzatives necessàries per preservar la seguretat de les dades personals i la seva no afectació als drets i les llibertats de les persones físiques. En aquest cas no cal passar a l'AIPD.

RECOMANACIÓ: La GARTDP de l'AEPD

Indica que "si como resultado del análisis previo se considera que no es necesario llevar a cabo una AIPD, se deben documentar adecuadamente los motivos por los cuales se ha llegado a esa conclusión", deixant constància que "se ha llevado a cabo ese análisis (responsabilidad proactiva)"

CARÀCTER DE LES AIPD:

"Las EIPD están orientadas a asegurar preventivamente que, cuando las operaciones de tratamiento puedan comportar riesgos espacialmente relevantes (alto riesgo), se tomen las medidas para reducir, dentro de lo posible, el riesgo de dañar o perjudicar a las personas, o afectar negativamente sus derechos y libertades, impidiendo o limitando su ejercicio o contenido"

Guia sobre l'avaluació d'impacte relativa a la protecció de dades al RGPD 2.0 (GPAI, en endavant), Barcelona, gener, 2018.

http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/Guia-sobre-la-evaluacion-de-impacto-relativa-a-la-proteccion-de-datos-en-el-RGPD/

AIPD EN TRACTAMENTS D'ALT RISC:

CONSIDERANT 84 RGPD:

"***A fin de mejorar el cumplimiento del presente Reglamento*** en aquellos casos en los que sea probable que las ***operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas***, debe incumbir al responsable del tratamiento la ***realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo***. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento".

QUAN DUR A TERME UNA AIPD?

CONSIDERANT 89 "in fine" RGPD

"Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial".

El considerant 90, per la seva banda, detalla què són "operacions a gran escala" i en quines altres operacions (arran, per exemple, del tractament de "dades de categories especials") es requereix AIPD.

REGULACIÓ DE L'AIPD EN L'RGPD

El marc regulador de l'AIPD es trova recollit per l'important article 35 RGPD. I l'article 36 RGPD recull el tràmit de "consulta prèvia" estretament relacionat amb els tractaments d'alt risc.

L'article 35.1 RGPD estableix una regla general que convé tenir sempre present: **"**Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares".

Per la seva banda, **l'article 35.3 determina en quins casos l'AIPD és necessària en els tractaments:**

- Avaluació sistemàtica i exhaustiva d'aspectes personals en un tractament automatitzat (elaboració de perfils) sobre la base dels quals es prenguin decisions que produeixin efectes jurídics. En aquest sentit caldria preguntar-se fins a quin punt és possible aprofitar els avantatges que proporciona l'Administració electrònica, ser proactius i utilitzar l'intercanvi de dades personals entre administracions públiques per oferir, per "anticipació", determinats serveis o prestacions a la ciutadania. Un cop més, en aquests casos, cal tenir en compte tot el que s'ha dit anteriorment

- Tractament a gran escala de "categories especials de dades"

- Observació sistemàtica a gran escala d'una zona d'accés públic

L'AIPD ha d'incloure, com a mínim, les exigències recollides per l'article 35.7 de l'RGPD (vegeu més endavant)

Altres qüestions:

- Per dur a terme l'AIPD el responsable comptarà sempre amb l'assessorament de la figura del delegat de dades personals (article 35.2).

- Cal tenir en compte en aquesta matèria les facultats de les autoritats de control (article 35, apartats 4, 5 i 6)

- El compliment de codis de conducta s'ha de tenir degudament en compte en avaluar les repercussions de les operacions realitzades pels responsables o encarregats (article 35.8 RGPD).

RÈGIM DE LA CONSULTA PRÈVIA: Regulació article 36 RGPD.

- Davant de qui es formula: Autoritat de control

- En quins casos: quan l'AIPD mostri que el tractament comporta alt risc

- Paper de l'autoritat de control: article 36, apartats 2 i 3. Vegeu així mateix apartat 4

PER SABER-NE MÉS; UN MATERIAL DE CONSULTA IMPRESCINDIBLE:

L'Autoritat Catalana de Protecció Dades ha publicat recentment una interessant i completa *Guía Práctica sobre la Evaluación de Impacto relativa a la Protección de Datos 2.0* (GPAI, en endavant), Barcelona, gener, 2018.

http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/Guia-sobre-laevaluacion-de-impacto-relativa-a-la-proteccion-dedatos-en-el-RGPD/

ALGUNS ADVERTIMENTS PRELIMINARS SEGONS L'AEPD SOBRE TRACTAMENTS ANTERIORS A L'ENTRADA EN VIGOR DE L'RGPD:

Guía Práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD (GEIPD)

1. "El RGPD prevé que las Evaluaciones de Impacto se lleven a cabo "antes del tratamiento" en los casos en que sea probable que exista un alto riesgo para los derechos y libertades de los afectados. Ello implica que el mandato del Reglamento no se extiende a las operaciones de tratamiento que ya estén en curso en el momento en que comience a ser de aplicación.

2. Sin embargo, sí debiera realizarse una Evaluación cuando en una operación iniciada con anterioridad a la aplicación del Reglamento se hayan producido cambios en los riesgos que el tratamiento implica en relación con el momento en que el tratamiento se pudo en marcha.

3. Este cambio en los riesgos puede derivar, por ejemplo, del hecho de que se hayan empezado a aplicar nuevas tecnologías a ese tratamiento, de que los datos se estén usando para finalidades distintas o adicionales a las que se decidieron en su momento, o de que se estén recogiendo datos distintos o diferentes",

ALGUNES LÍNIES FORÇA DE LA GEIPD (AEPD) I DE LA GPAI (apdCAT):

- **ALERTA PERMANENT:** "El continu avanç de la tecnologia i l'evolució dels tractaments propicien l'aparició contínua de nous riscos que han de ser gestionats: l'RGPD exigeix que els responsables del tractament implementin mesures de control"

- **AIPD:** "L'AIPD és una eina de caràcter preventiu". S'ha de reduir el nivell de risc a través de determinades mesures de control "fins a un nivell considerat acceptable".

- **QUAN S'HA DE FER UNA AIPD?:** Supòsits de "riscos elevats". L'AIPD està molt vinculada a dos conceptes: "alt risc" i tractament "a gran escala"

- **PRIVACITAT:** L'AIPD està alineada amb el principi de privacitat i ha de complir a més amb els principis de necessitat i proporcionalitat.

- **QUÈ HA D'INCLOURE UNA AIPD?:**

    - Una descripció sistemàtica de les activitats de tractament previstes

    - Una avaluació de la necessitat i proporcionalitat del tractament respecte a la seva necessitat

    - Una avaluació dels riscos

    - Les mesures per afrontar aquests riscos (garanties, mesures de seguretat i mecanismes que garanteixin la protecció de dades personals).

    - Fases:

        - Descriure el cicle de vida de les dades

        - Analitzar la necessitat i proporcionalitat de les dades

        - Gestió de riscos: Identificar amenaces i riscos; avaluar riscos; i tractar riscos

        - Pla d'acció i conclusions. Si escau, consulta prèvia

- **COM S'HA D'ENTENDRE L'AIPD:** S'ha d'entendre com un procés de millora contínua, "de manera que aquesta es revisi sempre que es modifiqui o actualitzi qualsevol aspecte rellevant de les activitats de tractament".

- **QUI HA DE REALITZAR L'AIPD:** El responsable del tractament. Però:

    - Tot i això, "és important destacar que la responsabilitat del 'responsable' no implica que l'àrea indicada per a cada fase de l'AIPD sigui obligatòriament qui hagi d'executar les tasques associades, podent recolzar-se en altres àrees, experts, recursos externs, etc."

    - L'obligació del fer una AIPD correspon al responsable del tractament, amb el suport i la col·laboració de l'encarregat del tractament i amb el DPD.

    - "Addicionalment, el personal encarregat de la seguretat, l'àrea de tecnologia, assessoria jurídica o fins i tot diferents responsables de diferents àrees implicades en el tractament poden ser requerides durant el procés d'avaluació"

RECOMANACIÓ GPAI (apdCAT):

"La documentación relacionada con las evaluaciones de impacto debe estar a disposición de las autoridades de supervisión, es decir, no solo el informe final, sino también el conjunto de trabajos que se han utilizado para hacer la evaluación y que sustentan las decisiones tomadas" (pàg. 15) [en castellano en el original]

- **QUIN ÉS EL PAPER DEL DELEGAT DE PROTECCIÓ DE DADES A L'AIPD?** El paper del delegat de protecció de dades a la AIPD és molt rellevant. A saber:

    - Proporciona l'assessorament necessari al responsable del tractament per a l'adequat desenvolupament de l'execució de l'AIDP.

    - "Suposa un valor afegit en el desenvolupament de l'AIPD aportant garanties per als drets i llibertats dels interessats".

    - "Hi pot haver estat el mateix delegat de protecció de dades qui hagi definit com s'ha d'executar les AIPD en l'organització (per exemple, mitjançant l'elaboració d'una guia interna d'avaluació o adoptant una guia externa que serveixi de marc d'avaluació); i així mateix, qui executi l'avaluació" (GPAI)

    - El DPD ha de verificar l'adequada execució de l'AIPD

- **METODOLOGIA** (Vegeu GEIPD, pàg. 10-36):

    - Context del tractament: Conèixer cicle de vida i flux de les dades

    - Gestió de riscos:

        - Identificar

        - Avaluar

        - Tractar

    - Comunicació i consulta a l'autoritat de control

    - Supervisió i revisió de la implantació: paper del DPD.

ORIENTACIONS PER A L'EXECUCIÓ DE L'AIPD SEGONS LA GPAI (APDCAT):

- **Aspectes preparatoris de l'execució de l'AIPD**: Mètode d'avaluació, interlocutors, equip d'avaluació, etc.

- **Anàlisi de la necessitat de fer l'AIPD**: quines dades es tractaran i de qui? (elaborar llista exhaustiva); volum de persones afectades pel tractament i si aquest és "a gran escala"; què es preveu fer amb les dades?

- **Descripció sistemàtica de les operacions de tractament** (descripció funcional segons el cicle de les dades)

- **Objectius i finalitats del tractament**: avaluació necessitat i proporcionalitat de les operacions de tractament

- **Gestió de riscos**: aspectes generals. Identificació de potencials escenaris de risc (PER)

- **Informe d'avaluació**: conclusions i recomanacions per mitigar els riscos de les operacions de tractament

IDEA FORÇA:

"La gestión de riesgos que prevé el RGPD va más allá de evaluar la exposición al riesgo de los sistemas de información o de los datos o de los riesgos para la organización" (GPAI/APDCAT, pàg. 61).

IDENTIFICACIÓ DE SITUACIONS DE RISC SEGONS RGPD GPAI/APDCAT (pàg. 61):

- Es priva els interessats dels seus drets i llibertats, que inclou quan s'impedeix el seu exercici normal i lliure
- Es provoquen danys i perjudicis físics, materials o immaterials a les persones interessades
- Es revelen categories especials de dades personals, o relatives a condemnes i infraccions penals, durant el tractament
- Es creen o s'utilitzen perfils personals
- Es tracten les dades personals de col·lectius especialment vulnerables
- Es tracta d'una gran quantitat de dades personals o dades que afecten un gran nombre de persones

QUATRE QÜESTIONS CLAU EN UNA AIPD (GEIPD, AEDP):

1. En cap cas es pot procedir a dur a terme un tractament si el risc és elevat

2. En aquells casos en què es presta un servei com a encarregat de tractament es recomana fer una anàlisi de riscos sobre la tipologia del servei prestat

3. Sempre que hi hagi una variació rellevant en el context de les activitats de tractament que pugui suposar un increment del risc associat al mateix, s'ha de fer una actualització de l'AIPD.

4. Si el responsable del tractament està adherit a algun codi de conducta on s'inclogui metodologia pròpia, es podrà utilitzar la mateixa per a la realització de les AIPD.

PER SABER-NE MÉS:

GT29 WP 248; *Directrices sobre la evaluación de impacto relativa a la protección de datos (AIPD) y para determinar si el tratamiento entraña probablemente un alto riesgo a efectos del Reglamento (UE) 2016/279* (En castellano en el original)

http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/altres_documents_del_grup_de_larticle_29/

IDEA-FORÇA FINAL:

Una AIPD és un procés utilitzat per a reforçar i demostrar el compliment (GPAI/adpCAT, pàg. 7)

SMART CITIES: UN EXEMPLE D'AIDP SEGONS L'AEPD

- « Antes de la puesta en producción de un proyecto Smart City es necesario hacer un análisis previo del mismo valorando el volumen de la información que se pretende procesar y el número y tipo de fuentes desde la que se pretende obtener dicha información o incluso el tiempo durante el que se pretende conservar esta información"

- Per tant en aquests casos, "será necesaria la realización de una evaluación de impacto relativa a la protección de datos o incluso una consulta previa a la autoridad de protección de datos" (p. 24)

AEPD, *Protección de datos y Administración Local, 2018.*

El delegat de protecció de dades

La figura del delegat de protecció de dades (DPD) és nova, encara que té alguns precedents que ara no cal esmentar.

S'insereix, com una peça més i important, al nou sistema institucional i de gestió de dades personals que s'emmarca en aquesta política "proactiva", anticipatòria o preventiva per la qual advoca l'RGPD.

Per a les administracions locals la nota més important és l'obligatorietat que estableix l'RGPD: totes elles han de disposar d'un DPD.

Realment, aquesta exigència, com tantes altres que conté l'RGPD, anava més dirigides a les administracions públiques de grans dimensions i d'altres sectorials on els riscos, l'ús massiu i les categories especials en el tractament de dades personals són la moneda corrent. Però l'obligació normativa hi és i, per tant, ha de complir-se.

Cal inserir la figura del DPD en aquest canvi de model de gestió de dades personals a què es ve fent referència. I **cal veure-ho com una finestra d'oportunitat, ja que el DPD hauria de contribuir en aquest procés de transformació organitzativa al canvi en els tractaments que l'RGPD exigeix.**

Aquesta transformació o trànsit d'una cultura "reactiva" a una altra "proactiva" no és fàcil, menys encara en un sector públic en el qual l'enduriment del règim sancionador de l'RGPD es veu fins a cert punt descafeïnat, al descansar principalment sobre "multes administratives".

En aquest context, **el DPD ha de ser una palanca de transformació que faci possible la implantació de la cultura proactiva també** en les institucions públiques i, pel que ara interessa, **en l'Administració local.**

Però, a més, el DPD és important que tingui coneixements especialitzats i qualificació pertinent, ja que és el punt de suport principal del responsable i de l'encarregat del tractament, a l'efecte de complir degudament les obligacions de l'RGPD. Hauria d'actuar, per tant, com un "tallafocs" que impedís incompliments. **Especialment important és el seu paper en els processos d'avaluació d'impacte.**

És en el considerant 97 on es dibuixen les línies mestres d'aquesta nova figura del DPD, que després seran desenvolupades pels articles 37 a 39 de l'RGPD, així com a través de referències incidentals (algunes que ja s'han vist) al llarg del resta de l'articulat.

CONSIDERANT 97 RGPD:

"Al supervisar la observancia interna del presente Reglamento, ***el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública,*** a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial (…) ***Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente."***

Quatre són, per tant, les idees-força que cal ressaltar del DPD segons aquest considerant 97

1. El DPD és un **col·laborador necessari**, tot i que també supervisor, del responsable o encarregat del tractament en el sector públic

1. Ha de ser DPD una persona que acrediti **coneixements especialitzats del dret i de la pràctica de protecció de dades**

1. El DPD pot ser **empleat públic o ser proveït de forma externa**

1. El DPD **exerceix les seves funcions i comeses "de manera independent"**

Abans d'endinsar-nos en l'anàlisi de la regulació normativa i en alguns aspectes operatius o pràctics que planteja a curt termini aquesta figura, és convenient delimitar el seu abast en l'àmbit del que fins ara indeterminadament anomenem "sector públic"

Què cal entendre per "autoritat i organisme públic" segons l'RGPD

L'RGPD utilitza ***l'expressió "autoritat i organisme públic"*** a l'hora d'atribuir l'exigència de crear necessàriament la figura del DPD.

I què cal entendre per "autoritat i organisme públic" segons l'RGPD?

Aquesta és una noció que, com va exposar el Grupo de Trabajo del Artículo 29 en el document que tot seguit se cita (*Directrices sobre los delegados de protección de datos*), reenvia al dret intern dels estats membres.

I, per tant, hauria de ser la futura LOPD qui precisi el seu perímetre. De moment, la redacció que s'ha donat a l'article 34 PLOPD és senzillament frustrant, doncs seguim sense saber amb certesa quines entitats del sector públic són les que estan obligades a disposar d'aquesta figura del DPD.

Per resoldre el problema (almenys fins que la LOPD s'aprovi definitivament) es pot intentar acudir a l'article 77 PLOPD, on es regula quin és el "Règim aplicable a determinades categories de responsables o encarregats del tractament" que, per una raó de paral·lelisme, es podria estimar que

són les entitats que sí que tenen l'obligació de disposar d'un DPD. Pel que fa a l'àmbit local de govern, el perímetre d'aplicació d'aquest règim singular es projecta sobre les següents entitats:

Els ens que integren l'Administració local (ajuntaments, vegueries o diputacions, àrees metropolitanes, comarques, mancomunitats i entitats municipals descentralitzades)

- Els organismes públics i entitats de dret públic vinculades o dependents de l'Administració local (organismes autònoms i entitats públiques empresarials)

- Les fundacions del sector públic adscrites a ens locals

- Els consorcis adscrits a un ens local

Si es pot traslladar aquest esquema institucional a les entitats que estan obligades a disposar d'un DPD, això suposaria que les societats mercantils no tindrien aquesta obligació «ex RGPD», però que sí que podria ser exigida en els mateixos termes que a les empreses del sector privat quan hi concorren les circumstàncies previstes en l'RGPD.

Però no sembla tenir gaire sentit que s'inclogui les fundacions i no les societats mercantils de capital públic. Algunes d'elles porten a terme precisament tractament de dades de forma extensa i intensa (cal pensar, per exemple, en totes aquelles societats mercantils de capital públic que presten serveis informàtics de suport a l'entitat matriu).

PER SABER-NE MÉS:

Directrices sobre los delegados de protección de datos (DPD), adoptades el 13 de desembre de 2016. Revisades per última vegada i adoptades el 5 d'abril de 2017, Grup de Treball sobre la protecció de Dades de l'Article 29. 16/ES WP 243, rev. 1. http://apdcat.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres/altres_documents_del_grup_de_larticle_29/

La regulació d'aquesta figura es recull principalment en els articles 37 a 39 RGPD.

L'article 37, dedicat a "**la designació**" del DPD, preveu els extrems següents:

- **DESIGNACIÓ PRECEPTIVA:** quan ha de designar-se segons l'RGPD pel responsable del tractament preceptivament un DPD? (article 37.1 RGPD) El cas de les autoritats i organismes públics ja ha estat analitzat, la qual cosa no impedeix que qualsevol organització ho pugui designar voluntàriament o si així ho exigeix la legislació d'un estat membre (article 37.4 RGPD)
- **QUANTS DPD?:** pretén donar resposta a si és possible nomenar un o diversos DPD (per grup d'empreses o autoritat o organisme públic, atenent a "la seva estructura organitzativa i la seva mida" (article 37.2 i 3 RGPD)
- **ACREDITACIÓ COMPETÈNCIES PROFESSIONALS:** les exigències professionals i coneixements que ha d'acreditar qui sigui designat DPD, vinculades a les funcions de la figura (article 37.5 en relació amb article 39 RGPD)
- **INTERN O EXTERN?** el DPD podrà formar part de la plantilla o ser un extern a l'organització (contractació de serveis) (article 37.6 RGPD)
- **PUBLICITAT DEL DPD:** el responsable o encarregat de publicar (presumiblement a la pàgina web o al portal de transparència) les dades de contacte del DPD i els comunicaran a apdCAT

Per la seva banda, l'article 38 té com a objecte "**la posició**" del DPD en relació amb el responsable o encarregat del tractament:

- **COL·LABORADOR NECESSARI:** Es preveu una garantia de participació del DPD en "totes les qüestions relatives a la protecció de dades personals" (article 38.1 RGPD).
- **RECURSOS:** Se li han de facilitar al DPD els recursos necessaris per a l'acompliment de les seves funcions i per al manteniment dels seus coneixements especialitzats (formació) (article 38.2 RGPD)
- **ESTATUT INDEPENDÈNCIA:** Garantia per la qual no rebrà cap instrucció pel que fa a l'exercici de les seves funcions, no podent ser destituït ni sancionat pel seu acompliment, i rendint comptes al més alt nivell jeràrquic de l'organització (article 38.3 RGPD)
- **PUNT DE CONTACTE:** Els interessats podran posar-se en contacte amb el DPD en les qüestions relatives a les seves dades personals i a l'exercici dels seus drets (article 38.4 RGPD).
- **CONFIDENCIALITAT:** El DPD està obligat a mantenir el secret o confidencialitat per a l'exercici de les seves funcions (article 38.5 RGPD)
- **DPD "A TEMPS PARCIAL":** El DPD podrà exercir altres funcions sempre que no donin lloc a conflictes d'interès (article 38.6 RGPD)

I, finalment, l'article 39 RGPD defineix quines són, com a mínim, les funcions del DPD, vinculant-les totes elles especialment a "riscos associats a les operacions de tractament" (article 39.2 RGPD). A saber:

FUNCIONS DEL DPD SEGONS L'RGPD:

- Informar i assessorar el responsable o l'encarregat del tractament i els empleats sobre les obligacions de l'RGPD i del dret intern
- Supervisar el compliment del present RGPD, promoure la seva implantació en l'organització i impulsar la formació
- Oferir assessorament sobre l'AIPD i supervisar la seva aplicació
- Cooperar amb l'autoritat de control
- Actuar com a punt de contacte de l'autoritat de control

Per la seva banda, haurà de ser la futura LOPD qui completi

alguns dels perfils d'aquest règim jurídic de la figura del DPD definida per l'RGPD.

El PLOPD conté, per exemple, les previsions següents (articles 34 a 37):

- Obligació de comunicar a l'adpCAT en el termini de 10 dies les designacions, nomenaments i cessaments dels DPD
- adpCAT mantindrà una llista actualitzada de DPD que serà accessible per mitjans electrònics
- Per Reial decret s'establirà el procediment d'interconnexió de les llistes creades per les autoritats de control (adpCAT/APDCAT/AVPD).
- L'acreditació dels «requisits» exigits per l'RGPD pot fer-se, entre altres mitjans, a través de mecanismes voluntaris de certificació
- La remoció del DPD es podrà realitzar si incorregués en dol o negligència greu en l'exercici de les seves funcions, previ expedient disciplinari tramitat a l'efecte (sector públic)
- El DPD tindrà accés a totes les dades personals i processos de tractament
- Qualsevol vulneració rellevant en matèria de protecció de dades serà comunicada pel DPD al responsable o encarregat del tractament.
- Amb caràcter previ a la interposició d'una reclamació davant l'autoritat de control per part de l'interessat, aquest «"podrá dirigirse al DPD de la entidad contra la que se reclame". En aquest cas, el DPD "comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación"
- Si l'afectat presenta la reclamació davant l'adpCAT, aquesta pot remetre la reclamació al DPD per tal que respongui en el termini d'un mes. En cas de són resposta, continuarà el procediment.

ALGUNES DIRECTRIUS DE LES AUTORITATS DE CONTROL SOBRE LA FIGURA DEL DELEGAT DE PROTECCIÓ DE DADES:
El Delegado de Protección de Datos en las Administraciones Públicas
http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php

PER SABER-NE MÉS:
Rafael Jiménez Asensio, "*La figura del Delegado de Protección de Datos en las organizaciones públicas*", La Mirada Institucional
https://rafaeljimenezasensio.com/2018/03/20/la-figura-del-delegado-de-proteccion-de-datos-en-las-organizaciones-publicas-1/
Víctor Almonacid, "*El Delegado de Protección de Datos en la Administración Local*"
https://nosoloaytos.wordpress.com/2018/03/28/el-delegado-de-proteccion-de-datos-en-la-administracion-local-dpo/#more-13764
Concepción Campos Acuña, "*Los 7 imprescindibles en protección de datos para el ámbito local*", El Consultor de los Ayuntamientos y Juzgados, enero 2018

IDEES-FORÇA I PROBLEMES APLICATIUS DE LA IMPLANTACIÓ DE LA FIGURA DEL DPD A LES ADMINISTRACIONS LOCALS

QUANTS DPD HAN DE TERNIR LES AAPP?:
- Com a mínim un, en les administracions públiques d'una determinada grandària poden ser dos o més, segons sectors. Res no impedeix, però, que sigui un sol DPD amb una unitat o departament i actuant de forma descentralitzada.

ELS GOVERNS LOCALS PETITS O MITJANS HAN DE TENIR DPD?
- Necessàriament, però aquesta funció pot ser prestada per les diputacions, comarques o, si s'escau, a través de mancomunitats o per mitjà de convenis entre ens locals (horitzontals o verticals).

PODEN SER DPD ÒRGANS COL·LEGIATS?
- El GT-ART-29 ho desaconsella; l'accessibilitat requereix personalització.

HA DE SER EL DPD FUNCIONARI O EMPLEAT PÚBLIC?
- Preferentment sí, sempre que realitzi funcions d'autoritat (funcionari), però és posible una externalització dels serveis, encara que no d'aquelles funcions que directament o indirectament exerceixin potestats públiques. Les funcions de l'RGPD poden ser exercides per un extern (empresa o professional), però les que assigna el PLOPD poden plantejar més dubtes.

ÉS POSSIBLE QUE EL DPD DESENVOLUPI LES SEVES FUNCIONS A TEMPS PARCIAL? Sí, sempre que no es vegi sotmés a conflictes d'interès.

POSICIÓ DEL DPD I FUNCIONS: LA RELACIÓ TRIANGULAR DEL DPD

FUNCIONS DEL DPD:

- RGPD fixa funcions mínimes. Deriven de la seva relació "triangular"

- Atenció especial als riscos en les operacions de tractament

- Les funcions essencials són:

  - Assessorar el responsable i encarregat de tractament

  - Assessorar, orientar sobre anàlisi de risc i executar, fins i tot, els AIPD

  - Supervisar compliment RGPD

  - Cooperar amb l'autoritat de control

  - Actuar com a punt de contacte

  - Conèixer de les reclamacions prèvies protecció de dades i per remissió de l'autoritat de control (PLOPD)

QUALITATS PROFESSIONALS QUE HA D'ACREDITAR EL DPD:

- "Qualitats professionals i coneixements especialitzats":

  - Coneixements i experiència de Dret públic (Directrius: procediments administratius)

  - Coneixements i experiència de protecció de dades

  - Bon maneig de l'RGPD i de tots els instruments que recull el reglament

- Quin àmbit professional és el més idoni per al desenvolupament d'aquestes funcions?

  - No hi ha reserva professional. Però, el PLOPD li dona un biaix jurídic acusat: resoldre reclamacions (es pot esmenar amb personal tècnic adscrit)

  - Les Directrius afegeixen també integritat i ètica (incideixen molt en com evitar conflictes d'interessos).

ESTATUT JURÍDIC I POSICIÓ DEL DPD:

- Independència: no rep cap instrucció. No té dependència jeràrquica

- Participació primerenca en els processos de tractament de dades

- Presència en els òrgans que adopten decisions (problema amb externs)

- Proveir dels recursos necessaris si és intern (local, mitjans personals i tecnològics)

- Facilitar-li formació per al manteniment dels seus coneixements

- "Temps suficient" per a l'exercici de les seves funcions

- A major complexitat del tractament més recursos

- Rendició de comptes al màxim nivell (externs)

- Blindatge enfront de sancions (PLOPD) i remocions

- Mantenir secret i confidencialitat

UBICACIÓ ORGÀNICA DEL DPD:

- Com enquadrar-lo en l'estructura?

- Descartar el seu enquadrament com a alt càrrec

- Unitat situada a Alcaldia o a la Presidència. Motius

- Cobertura preferentment per funcionari A1. No necessàriament jurista

- Figura incardinada en el model de seguretat informàtica

ALGUNS PROBLEMES DE RRHH EN RELACIÓ AMB EL DPD: LLISTAT DE QÜESTIONS OBERTES

- Crear un lloc de treball "ad hoc" o acumular les funcions a un altre lloc existent

- Incorporar plantilla pressupostària i a l'RLT, si escau

- Com cobrir aquest lloc de treball?

  - Selecció "ex novo" desaconsellable. Raons

  - Cobrir-lo amb funcionaris interins, desaconsellable també

  - Es pot designar personal laboral? Planteja dificultats (PLOPD)

- La primera tensió: discrecionalitat i professionalitat. Ha de prevaler aquesta última: criteris de competència professional

- Provisió lloc DPD. modalitats

  - Lliure designació. Desaconsellada, no s'ajusta RGPD.

  - Concurs de mèrits, no mesura competència professional efectiva

  - Concurs específic, podria ser el més idoni

  - Seria possible la comissió de serveis i altres formes de provisió?

- La segona tensió: temporalitat versus permanència. Decisió estratègica: lloc d'estructura permanent, però cobert per períodes. No hi ha (gairebé) professionals amb aquest perfil. Importància estratègica.

  - Decisió complexa en un primer moment, tot i que RGPD sembla donar caràcter estructural de la figura, això no impediria rotació.

  - Dificultats, marc jurídic rígid.

  - Es podria explorar la figura de la DPP com una alternativa. Problemes: normativització.

ARBRE DE DECISIONS EN RELACIÓ AMB EL DPD A LES ADMINISTRACIONS LOCALS:

1.- Internalitzar o externalitzar la figura. Valorar "pros" i "contres". Prestar serveis per una altra administració (definició del conveni). Prestar serveis externs (definició plecs).

2.- Un o diversos DPD.

3.- Com i on enquadrar-la en l'estructura organitzativa. No dependència.

4.- Dotar-la de mitjans: estructura personal?

5.- A temps complet o parcial

6.- Quin règim jurídic apliquem?

7.- Quin sistema de provisió?

8.- Com salvaguardar la seva independència?

ALGUNES CONCLUSIONS:

- Figura singular i de complex encaix. Prova assaig/error

- Anirà creixent en protagonisme a mesura que avanci la revolució tecnològica

- Banc de proves per explorar la incorporació de nous perfils

- L'exigència d'inscripció es difereix a l'aprovació de la LOPD. Es guanya temps.

- Factor temps: Ens hem despertat molt tard i sense les eines necessàries

Codis de conducta i mecanismes de certificació

Es tracta de **dos instruments que entronquen perfectament amb l'enfocament "proactiu" que imprimeix l'RGPD.** Tenen, per tant, una orientació preventiva o anticipatòria.

Així mateix **són eines de caràcter voluntari,** però que en el cas dels codis de conducta, un cop assumits per aquells que s'adhereixin als mateixos tindran caràcter vinculant.

En qualsevol cas, sense perjudici del que es dirà, cal presumir que l'adhesió a aquests codis pot implicar l'atenuació en el seu cas de les responsabilitats derivades per un tractament de dades incorrecte. Encara que, en el supòsit dels mecanismes de certificació, expressament es recull la idea que la certificació no limitarà la responsabilitat del responsable o de l'encarregat (article 43.4 RGPD). Per aquest motiu es parlava a l'inici d'aquesta Guia d'una política de compliance atenuada traslladada a la protecció de dades.

CODIS, CERTIFICACIÓ I POLÍTICA DE COMPLIMENT

Aquesta impressió inicial pot esvair-se si s'analitzen aquestes eines en el marc del conjunt de previsions de l'RGPD.

En efecte, els trets del sistema preventiu i de compliment són evidents en certs passatges de l'RGPD. Tal com preveuen els articles 24.3 i 28.5 RGPD, l'adhesió a codis de conducta o mecanismes de certificació "pueden ser utilizados como elementos para demostrar el cumplimiento" o l'existència d'una sèrie de garanties, respectivament, per part del responsable o l'encarregat del tractament.

Així mateix, l'adhesió a un codi de conducta o a un mecanisme de certificació " podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos" (en matèria de seguretat) en l'article 32.1 RGPD (article 32.3 RGPD).

També el compliment dels codis de conducta "se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por los responsables o encargados", en particular quan es dugui a terme una AIPD.

IDEA-FORÇA:

Per tant, **disposar de codis de conducta i mecanismes de certificació** no és només adoptar una visió preventiva en línia amb la finalitat de l'RGPD, sinó especialment ***dotar-se d'una política de compliment que salvaguarda la funció del responsable o encarregat del tractament*** de qualsevol organització, també de l'Administració local.

REGULACIÓ CODIS DE CONDUCTA

En l'RGPD:

L'RGPD regula en els articles 40 a 43 els codis de conducta i els mecanismes de certificació. Malgrat el seu caràcter de lliure adhesió, cal constatar que algunes d'aquestes previsions no s'apliquen a "les autoritats i organismes públics".

L'article 40.1 RGPD preveu una tasca de promoció dels codis de conducta que serà duta a terme per l'adpCAT (o la resta d'autoritats de control), en la qual es tindran en compte les característiques específiques dels diferents sectors de tractament.

IDEA-FORÇA:

Els codis de conducta estan destinats a contribuir a la correcta aplicació de l'RGPD (article 40.1)

Per la seva banda, l'article 40.2 fa referència al fet que" las asociaciones y otros organismos representativos de categorías de responsables o encargados de tratamiento podrán elaborar códigos de conducta". Com podrien ser, per exemple, les associacions o federacions de municipis o ens locals, si escau.

I s'estableix un contingut orientatiu del que poden recollir aquests codis. Per exemple (Vegeu article 42.2 RGPD):

- La recollida de dades personals
- La informació proporcionada al públic i als interessats
- L'exercici dels drets de l'interessat
- Les mesures i procediments per garantir la seguretat del tractament
- La notificació i comunicació de les violacions de la seguretat de les dades, respectivament, a l'autoritat de control i als interessats

És important, així mateix, tenir en compte que les associacions que promoguin aquests codis de conducta (per exemple, FMC, ACM, FEMP o EUDEL) han de presentar el **projecte de codi davant l'autoritat de control** (adpCAT o l'autoritat que correspongui: AEPD o AVPD), perquè per part d'aquesta es dictamini si és conforme a l'RGPD i procedeixi a aprovar tal codi "si considera suficiente las garantías adecuadas ofrecidas". Per part de l'autoritat de control es registrarà i publicarà l'esmentat codi (article 40.5 i 6 RGPD).

ACLARIMENT (Exclusió autoritats i organismes públics):

Cal tenir en compte que l'article 41 RGPD («Supervisió dels codis de conducta aprovats»), així com per connexió l'article 40. 4 RGPD, no s'aplicaran al tractament realitzat per autoritats i organismes públics (article 41.6 RGPD)

En el PLOPD

La regulació (provisional) dels codis de conducta que conté el PLOPD en el seu article 38 té els següents trets:

- Els codis de conducta seran vinculants per a tots aquells que s'hi adhereixin.
- Podran ser promoguts per associacions i organismes, però també pels responsables o encarregats a què es refereix l'article 77.1 LOPD. Per tant, per qualsevol ens local, organisme públic, consorci o fundació.
- Els codis seran aprovats per les autoritats de control (adpCAT/AEPD/AVPD)
- Les autoritats de control hauran de sotmetre els projectes de codi de conducta al mecanisme de coherència que estableix l'article 63 RGPD, en relació amb el que preveu l'article 40.7 RPD.
- L'Agència Espanyola de Protecció de Dades i les autoritats autonòmiques de protecció de dades mantindran un registre conjunt dels codis de conducta aprovats.

- Per Reial decret s'establirà el contingut del registre i les especialitats del procediment d'aprovació dels codis de conducta.

REGULACIÓ MECANISMES DE CERTIFICACIÓ

En l'RGPD

En el artículo 42.1 también se recoge una labor de "promoción" que debe ser ejercida entre otros por los Estados miembros y las autoridades de control con la finalidad de crear mecanismos de certificación en materia de protección de datos y sellos y marcas de protección de datos. El objetivo de tales instrumentos es siempre "demostrar el cumplimiento de lo dispuestos en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados"

Els articles 42 i 43 RGPD regulen els mecanismes i organismes de certificació.

L'article 42.1 recull que una tasca de "promoció" ha de ser exercida entre d'altres pels estats membres i per les autoritats de control amb la finalitat de crear mecanismes de certificació en matèria de protecció de dades i segells i marques de protecció de dades. L'objectiu d'aquests instruments és sempre «demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados"

IDEA-FORÇA:

Els mecanismes de certificació (segells o marques) tenen com a finalitat principal demostrar que, per part dels responsables i encarregats del tractament, es compleix l'RGPD. Tendeixen, per tant, a salvaguardar l'actuació de responsables i encarregats. D'aquí la importància de dotar-se d'aquestes eines.

Las línies bàsiquesd'aquesta regulació són les següents:

- La certificació serà voluntària i estarà disponible a través d'un procés transparent (article 42.3 RGPD)

- La certificació no limitarà les responsabilitat del responsable o encarregat del tractament pel que fa al compliment del present Reglament (article 42.4 RGPD)

- Serà expedida pels organismes de certificació que regula l'article 43 RGPD o per l'autoritat de control competent (adpCAT), sobre la base de criteris aprovats per aquesta autoritat en els termes que estableix l'article 42 RGPD

- Obligació dels responsables i encarregats del tractament de proveir tota la informació necessària per dur a terme el procediment de certificació

- La certificació serà expedida al responsable o encarregat del tractament per un període màxim de tres anys, renovables en les condicions exposades (article 42.6 RGPD)

En el PLOPD

L'article 39 PLOPD confereix la competència per a dur a terme l'acreditació de les institucions de certificació a l'Entitat Nacional d'Acreditació (ENAC), que serà la que comuniqui a les autoritats de control respectives (adpCAT) les concessions, denegacions o revocacions de les acreditacions, així com la seva motivació.

Així mateix, s'ha de tenir en compte la disposició transitòria segona del PLOPD en relació amb els codis tipus inscrits en les autoritats de protecció de dades de conformitat amb el que estableix la Llei orgànica 15/1999, de 13 de desembre: adaptació del seu contingut a l'article 40 RGPD en el termini d'un any.

UNA BONA PRÀCTICA:

Esquema de Certificación de Delegados de Protección de Datos de l'Agència Espanyola de Protecció de Dades (Esquema AEPD-DPD)

http://www.agpd.es/portalwebAGPD/temas/certificacion/index-ides-idphp.php

Autoritats de control independents: Idea general

No hi ha dubte que la correcta implantació de l'RGPD, també en els diferents nivells de govern (i, en particular, en l'Administració local) requereix d'aquesta peça institucional imprescindible que són les autoritats de control.

No és objecte d'aquesta Guia, per les seves especials característiques, analitzar el paper i funcions de tals autoritats de control, a les quals l'RGPD i el PLOPD dediquen un bon espai regulador.

En aquestes pàgines només interessa destacar quina és la finalitat de les autoritats de control, especialment de l'adpCAT (encara que també les seves relacions amb l'AEPD i amb l'AVPD), i posar en relleu alguns dels seus elements més rellevants, ja que es tracta sens dubte, del mecanisme de tancament perquè el nou sistema institucional i de gestió de protecció de dades de les administracions locals funcioni correctament.

Sota aquest punt de vista és oportú ressaltar que la finalitat principal de les autoritats de control no és una altra que la protecció de les persones físiques pel que fa al tractament de dades de caràcter personal. Aquesta és una idea que es recull perfectament en el considerant 117 i en altres successius (per exemple, en el considerant 123 on s'afegeix a la finalitat anterior la de "facilitar la libre circulación de los datos personales en el mercado interior"). En l'exercici d'aquestes funcions "deben supervisar la aplicación de las disposiciones adoptadas de conformidad con el presente Reglamento y contribuir a su aplicación coherente en toda la Unión".

CONSIDERANT 117 RGPD

"El establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa".

No interessa abordar aquí les qüestions relatives a la posició institucional d'aquestes autoritats de control ni tampoc a l'existència de diverses autoritats de control o la designació, en aquest cas, d'una autoritat de control que exerceixi com a "punt de contacte únic" (considerant 117). Però, sí que pot ser oportú ressaltar que les àmplies comeses funcionals que l'RGPD encomana a tals autoritats de control implicaran necessàriament un reforç de recursos financers i humans, que no sembla ser molt viable en època de contenció fiscal.

REGULACIÓ DE LES AUTORITATS DE CONTROL A L'RGPD

La regulació de les autoritats de control a l'RGPD la resumeix el capítol VI. Aquest capítol s'estructura en diferents seccions que aborden, entre d'altres, els àmbits materials següents:

- Designació d'una o diverses autoritats per Estat (actualment a Espanya n'hi ha tres: AEPD, adpCAT i AVPD) (article 51 RGPD)
- Estatut d'independència de les esmentades autoritats (alienes a tota influència externa, ja sigui directament o indirecta i no admetran cap instrucció) (article 52 RGPD)
- Condicions aplicables als membres de les autoritats de control i normes relatives a l'establiment de l'autoritat de control (articles 53 i 54 RGPD)
- Competències de l'autoritat principal de control (articles 55 i 56 RGPD)
- Funcions és l'aspecte més important als nostres efectes i es tracta de forma singularitzada (article 57 RGPD)
- Poders, que es desdoblen en poders d'investigació, correctius o d'autorització i consultius (article 58 RGPD)
- Informe d'activitat (article 59 RGPD)

ALGUNES FUNCIONS DE LES AUTORITATS DE CONTROL EN RELACIÓ AMB ELS GOVERNS LOCALS:

- Controlar l'aplicació d'aquest Reglament i fer efectiva la seva aplicació

- Assessorar les institucions sobre les mesures administratives que cal adoptar per a la protecció dels drets i llibertats pel que fa al tractament de dades

- Promoure la sensibilització dels responsables i encarregats del tractament sobre les seves obligacions derivades del present Reglament

- Tractar les reclamacions presentades

- Dur a terme investigacions sobre l'aplicació del present Reglament

- Adoptar clàusules contractuals tipus

- Elaborar una llista relativa al requisit d'avaluació d'impacte

- Oferir assessorament sobre operacions de tractament

- Animar per a l'elaboració de codis de conducta, dictaminar-los i aprovar-los

- Fomentar la creació de mecanismes de certificació de la protecció de dades i aprovar els criteris de certificació

- L'acompliment de les funcions de l'autoritat de control serà gratuït per a l'interessat i pel delegat de protecció de dades; llevat de les excepcions taxades a la norma (article 57.4 RGPD).

ALGUNS "PODERS CORRECTIUS" DE LES AUTORITATS DE CONTROL SEGONS L'RGPD

- Sancionar tot responsable o encarregat del tractament amb un advertiment

- Ordenar al responsable o encarregat del tractament que atengui les sol·licituds d'exercici dels drets de l'interessat en virtut de l'RGPD

- Ordenar al responsable o encarregat del tractament que les operacions de tractament s'ajustin a l'RGPD

- Ordenar al responsable de tractament que comuniqui les violacions de la seguretat de les dades personals

- Imposar una limitació temporal o definitiva del tractament, inclosa la seva prohibició

- Ordenar la rectificació o supressió de dades personals o la limitació de tractament

- Retirar un certificat

- Imposar una multa administrativa (vegeu règim singular entitats sector públic)

REGULACIÓ DE LES AUTORITATS DE CONTROL EN EL PLOPD

El títol VII del PLOPD regula exhaustivament les autoritats de protecció de dades.

No pot ser objecte d'aquesta Guia una anàlisi detinguda d'aquestes previsions, i més el caràcter provisional que tenen ja que es troben en plena tramitació d'esmenes del projecte de llei.

Per tant, només es donarà notícia puntual d'alguns dels punts d'aquesta proposta normativa a l'efecte de pura informació i, òbviament, d'aquells que puguin afectar amb més intensitat les entitats locals.

Alguns aspectes d'interès d'aquesta regulació a l'efecte de la present Guia serien els següents:

- En el capítol relatiu a l'Agència de Espanyola de Protecció de Dades, convé ressaltar el següent:
    - En l'àmbit de les potestats d'investigació i plans d'auditoria preventiva cal tenir en compte el que disposa l'article 51 sobre l'àmbit de la investigació i personal competent per a dur-la a terme.
    - Igualment és important el deure de col·laboració de les administracions públiques que estableix l'article 52.
    - Les potestats de regulació a través de "Circulars de l'Agència Espanyola de Protecció de Dades"
    - O les funcions relacionades amb l'acció exterior.
- En el capítol relatiu a les autoritats autonòmiques de protecció de dades, es contenen algunes previsions importants en l'àmbit local. Per exemple, dues d'elles vinculades amb l'exercici que a aquests autoritats de control se'ls reconeixen les funcions establertes en els articles 57 i 58 RGPD, quan es refereixin a:
    - Tractaments dels quals siguin responsables les entitats integrants del sector públic de la comunitat autònoma de les entitats locals incloses en el seu àmbit territorial o aquells que prestin serveis a través de qualsevol forma de gestió directa o indirecta.
    - Tractaments duts a terme per persones físiques o jurídiques per a l'exercici de les funcions públiques en matèries que siguin competència de la corresponent administració autonòmica o local.
- Cal presumir igualment que la normativa reguladora de les autoritats de control de les comunitats autònomes (adpCAT i AVPD, així com, si és el cas, ATPDA) s'han d'adaptar al que estableix l'RGPD.

Règim de responsabilitats i sancions: Idea general. Aplicació al sector públic

Un dels pilars d'aquesta nova regulació era dotar la normativa (i, en particular, a les autoritats de control) de "poders coercitius més contundents" per tal de protegir els drets i llibertats de les persones físiques com a conseqüència dels tractaments de dades personals. Darrere de tot això està, sens dubte, l'avenç imparable de la revolució tecnològica i el poder quasi absolut de les empreses d'aquest mateix àmbit que despleguen la seva activitat amb el maneig i encreuament de tota la informació recuperada a través dels motors de cerca, de les xarxes socials o dels correus electrònics.

Amb aquesta finalitat d'enfortir l'aplicabilitat del nou marc normatiu en aquesta matèria, no quedava una altra opció que fer tot l'èmfasi que fos necessari en el poder sancionador. I aquesta és una qüestió que es recull en els considerants 149 i següents de l'RGPD. Vegeu un exemple.

CONSIDERANT 148 RGPD

"A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías".

En tot cas, com anuncia el títol del present epígraf, la pretensió d'aquestes línies és només donar una idea general d'aquesta problemàtica, entre altres coses perquè la seva aplicabilitat a les entitats del sector públic es veu mediatitzada per la regulació prevista al PLOPD, on -malgrat el canvi qualitatiu que implica l'RGPD- en l'àmbit sancionador segueix l'antic patró de la LOPD de 1999, amb alguns matisos.

REGULACIÓ EN L'RGPD

El capítol VIII de l'RGPD s'enuncia de la manera següent: "Recursos, responsabilitat i sancions". D'aquesta regulació ens interessa particularment tot allò que té a veure amb la responsabilitat i el règim de sancions. Però, molt succintament, aquest capítol aborda els següents temes:

- Preveu el dret que té tot interessat de presentar una reclamació davant l'autoritat de control si considera que el tractament de dades personals aplicat infringeix el present Reglament (article 77)

- Així mateix, preveu el dret a la tutela judicial efectiva en un doble sentit: contra una autoritat de control; i contra un responsable o encarregat del tractament (articles 78-79)

- Regula la representació dels interessats (article 80) i la suspensió dels procediments (article 81)

- Es conté una important regulació relativa al dret d'indemnització i responsabilitat (article 82), de la qual convé destacar alguns extrems.

- Cal tenir en compte que aquest capítol VIII, sobretot el seu article 83, reenvia a determinats "poders" (amb implicacions òbviament sancionadores) que exerceixen les autoritats de control segons l'article 58 (per exemple, advertències).

- L'article 83 estableix el que ha denominat "Condicions generals per a la imposició de multes administratives". Un precepte fonamental a partir del qual la legislació dels estats membres adaptarà el seu règim sancionador o l'haurà d'imposar en aquells casos en que no en tingués. Particularment important pel què es dirà és l'article 83.7 RGPD. Aquest precepte requereix així mateix una cita expressa.

DRET A INDEMNITZACIÓ I RESPONSABILITAT: EXTRACTES (ARTICLE 82 RGPC)

1. ***"***Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.
2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable".

CONDICIONS GENERALS PER A LA IMPOSICIÓ DE MULTES ADMINISTRATIVES: EXTRACTES (ARTICLE 83)

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.
2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta: (...)
3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.
4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía: (...)
5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía: (...)"

LA PREVISIÓ PUNTUAL PER A LES AUTORITATS I ORGANISMES PÚBLICS: ARTICLE 83.7 RGPD

7. ***"***Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, ***cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro"***

PROPOSTA DE REGULACIÓ EN EL PLOPD

El títol IX del PLOPD tracta del règim sancionador. I molt breument ens interessa fer esment a alguns d'aquests articles, però especialment la previsió recollida en l'article 77 PLOPD, perquè –en cas que s'aprovés en aquests termes la futura LOPD- col·locaria a les entitats del sector públic en una posició gairebé similar a la que es troba actualment l'Administració pública en el marc normatiu vigent anterior a l'RGPD.

En termes generals, la regulació que es proposa conté els següents elements:

- Subjectes responsables (article 70 PLOPD), on es preveuen entre d'altres els responsables i els encarregats dels tractaments, així com s'afirma que al delegat de protecció de dades no li és aplicable el règim sancionador previst en aquest títol.

- Es tipifiquen les infraccions molt greus, greus i lleus (respectivament, articles 72, 73 i 74)

- Es regula la interrupció de la prescripció (article 75) i el règim de prescripció de les sancions (article 78)

- També es recull una regulació sobre sancions i mesures coercitives.

- I, finalment, l'article 77 del PLOPD estableix un «règim aplicable a determinades categories de responsables o encarregats del tractament», amb empara en l'article 83.7 RGPD. I, donada la seva importància per a l'Administració local, és oportú reproduir-lo en la seva integritat, al marge de com quedi realment en la versió final després de la seva tramitació parlamentària.

ARTICLE 77 PLOPD: Règim aplicable a determinades categories de responsables o encarregats del tractament.

1. "El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.

b) Los órganos jurisdiccionales.

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

e) Las autoridades administrativas independientes.

f) El Banco de España.

g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.

h) Las fundaciones del sector público.

i) Las universidades públicas

j) Los consorcios".

2. "Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 73 a 75 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos podrá proponer también la iniciación de actuaciones disciplinarias. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, ésta publicará en su página web con la debida separación las resoluciones en que se imponga una sanción a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción".

PER SABER-NE MÉS:

GRUP DE TREBALL SOBRE LA PROTECCIÓ DE DADES DE L'ARTICLE 29; 17/ES WP 253

Directrices sobre la aplicación y fijación de multas administrativas a efectos del Reglamento 2016/679

Altres qüestions. Situacions específiques de tractament

Amb caràcter merament telegràfic convé posar en relleu algunes altres disposicions que l'RGPD enquadra com a "situacions específiques de tractament".

A tal efecte, s'hauran de tenir en compte les següents previsions:

- **Tractament i llibertat d'expressió i informació** (article 85 RGPD), la qual cosa implica una obligació als estats membres per conciliar la protecció de dades personals amb aquest dret fonamental, en particular pel que fa al tractament amb finalitats periodístiques i d'expressió acadèmica, artística o literària.

- En l'article 86 RGPD es regula el **tractament i accés a documents oficials.**

- Per la seva banda l'article 87 preveu una **regulació del nombre nacional d'identificació.**

- L'article 89 preveu una sèrie de **garanties aplicables al tractament amb finalitats d'arxiu en interès públic, finalitats d'investigació científica o històrica i finalitats estadístiques.**

- L'article 90 s'ocupa de les **obligacions de secret.**

- I, finalment, l'article 91 té per objecte les **«normes vigents sobre protecció de dades de les esglésies i associacions religioses».**

- Particular importància té la previsió de l'article 88, sobre **tractament en l'àmbit laboral,** que cal entendre plenament aplicable a les relacions d'ocupació en l'àmbit del sector públic.

ARTICLE 88 RGPD:
TRACTAMENT EN L'ÀMBIT LABORAL

"1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral".

2. "Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.
3. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas".

En aquest sentit és de notable importància la proposta normativa recollida en la disposició addicional quinzena del PLOPD que té per objecte una sèrie de "disposicions específiques aplicables als tractaments dels registres de personal del sector públic".

Disposició addicional quinzena. Disposicions específiques aplicables als tractaments dels registres de personal del sector públic

"1. Los tratamientos de los registros de personal del sector público se entenderán realizados en el ejercicio de poderes públicos conferidos a sus responsables, de acuerdo con lo previsto en el artículo 6.1.e) del Reglamento (UE) 2016/679.
2. Los registros de personal del sector público podrán tratar datos personales relativos a infracciones y condenas penales e infracciones y sanciones administrativas, limitándose a los datos estrictamente necesarios para el cumplimiento de sus fines.
3. De acuerdo con lo previsto en el artículo 18.2 del Reglamento (UE) 2016/679, y por considerarlo una razón de interés público importante, los datos cuyo tratamiento se haya limitado en virtud del artículo 18.1 del citado reglamento, podrán ser objeto de tratamiento cuando sea necesario para el desarrollo de los procedimientos de personal".

Així mateix, pel que fa a la **transparència publicitat activa i al dret d'accés a la informació pública,** és important tenir en compte el que recull la disposició addicional segona del PLOPD que, en matèria de protecció de dades reenvia al que disposen els articles 5.3 i 15 de la Llei 19/2013, al que estableix l'RGPD i també al que reguli la LOPD. Aquesta referència s'ha d'entendre extensiva al que estableix la Llei 19/2014, del Parlament de Catalunya, de transparència, accés a la informació pública i bon govern.

DOCUMENTACIÓ RECENT AEDP: MOLT INTERESANT

Listado de cumplimiento normativo para facilitar la adaptación al RGPD

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2018/notas_prensa/news/2018_04_13-ides-idphp.php

Final

Protecció de dades i intel·ligència artificial

LES DADES NO SÓN EL NOU PETROLI DE L'ECONOMIA

"Uno de los lugares comunes de nuestro tiempo es que los datos son el nuevo petróleo (...) Pero los datos no se parecen al petróleo. El petróleo es un recurso finito; los datos son infinitamente renovables"

(Franklin Foer, Un mundo sin ideas: La amenaza de las grandes empresas tecnológicas a nuestra identidad; Paidós, 2017, pp. 182-183)

L'ERA DE L'ALGORITME

"La era del algoritmo marca el momento en que la memoria técnica ha evolucionado para almacenar no solo nuestros datos, sino también algunos patrones del comportamiento más sofisticado, desde el gusto musical hasta nuestros grafos sociales. En muchos casos, ya nos estamos imaginando sincronizados con nuestras máquinas".

(Ed Finn, La búsqueda del algoritmo. Imaginación en la era de la informática, Alpha Decay, p. 336)

UNA IDEA PER AL DEBAT

"¿Y qué significa realmente la retórica en torno a la smart city o ciudad inteligente? Si se lee más de cerca, quiere decir que nuestra infraestructura urbana será entragada a un grupo de empresas tecnológicas (desde luego no muy propensas a la transparencia) que luego la gestionarán como mejor les parezca, lo que hará casi imposible remunicipalizarlas más adelante"

(Evgeny Morozov, Capitalismo Big Tech, Enclave, 2018, P. 269).

L'ÈTICA DE L'ALGORITME

"Puede que llegue el momento, quizás más pronto que tarde, de que la pregunta sobre la ética de los algoritmos deba plantearse con respecto a la inteligencia artificial en evolución o, incluso, deba dirigirse a esa mente-máquina. De momento, aún es esencialmente una pregunta para los seres humanos que escriben los algoritmos"

(Thimothy Garton Ash, Libertad de palabra. Diez principios para un mundo conectado, Tusquets Editores, 2017, p. 494).

PER SABER-NE MÉS:

Un document molt recent (9 abril 2018):
A Statement on Artificial Intelligence, Robotics and 'autonomous' systems by the European Group of Ethics and Science in New Technologies:

http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf

BONA PRÀCTICA

ELS NOUS REPTES DEL RGPD EN LA GESTIÓ I TRACTAMENT DE DADES DE CARÀCTER PERSONAL:

LA SEGURETAT INTEGRAL A L'AJUNTAMENT DE SANT FELIU DE LLOBREGAT

1. Contextualització i antecedents
2. La seguretat integral
3. Reorganització de la seguretat a l'ajuntament
4. Adequació al reglament general de protecció de dades
5. Conclusions

1. CONTEXTUALITZACIÓ I ANTECEDENTS

L'objecte d'aquest treball és compartir l'experiència de l'Ajuntament de Sant Feliu de Llobregat en el seu camí per a l'adaptació de la seva organització interna a les obligacions que, en matèria de seguretat i protecció de dades de caràcter personal, la normativa ha anat imposant a les Administracions Públiques.

L'Ajuntament de Sant Feliu de Llobregat porta molts anys adaptant la seva organització als requeriments que successivament ha anat imposant a les administracions públiques la regulació en matèria de protecció de dades de caràcter personal.

Establertes les bases organitzatives de l'època per a la correcta protecció de les dades de caràcter personal, una nova tanda de lleis administratives van donar un gir exponencial al que amb anterioritat tractava, d'una banda, la normativa de protecció de dades, i de l'altra, certs estàndards recollits en normes ISO, relatives a la seguretat dels sistemes.

Un primer revulsiu en aquesta matèria va ser l'aprovació de la Llei 11/2007 LAECSP, que recollia en el seu articulat la necessitat d'aguditzar la protecció de dades en l'activitat electrònica de les administracions públiques. De fet, aquest nou model d'Administració pública s'ha anat configurant, des de l'any 2007, mitjançant la publicació de normativa a nivell europeu, estatal i autonòmic, que reconeixen tot un conjunt de drets a la ciutadania i imposen obligacions a les Administracions públiques en matèria d'Administració electrònica (Lleis 39 i 40/2015, de procediment administratiu i règim jurídic del sector públic, i esquemes nacionals de seguretat i interoperabilitat); de transparència, accés a la informació pública i bon govern (Llei estatal 19/2013 i Llei catalana 19/2014); de simplificació de l'activitat administrativa de la Generalitat i dels governs locals de Catalunya (Llei 16/2015); de reutilització de la informació (Llei 37/2007, modificada per Llei 18/2015); de contractació electrònica (Llei 9/2017); de protecció de dades de caràcter personal (Reglament (UE) 2016/679 del Parlament Europeu i del Consell); entre d'altres.

Aquestes normatives incideixen en el compliment dels principis plasmats al Pla d'Administració Electrònica 2016-2020 de la Unió Europea, que té com a objectiu principal **eliminar els obstacles digitals** que s'oposen al Mercat Únic Digital i evitar la fragmentació que es pot generar en el context de transformació de les administracions públiques.

Aquests principis es concreten en les següents dimensions:

- **Digital per defecte,** les AAPP oferiran serveis digitals com a opció preferent.
- **Principi d'una sola vegada,** garantint que la ciutadania i empreses subministren la mateixa informació només una vegada a les AAPP.
- **Inclusió i accessibilitat** de forma predeterminada.
- **Obertura i transparència,** garantint que la ciutadania i empreses puguin tenir control d'accés i rectificació de les seves pròpies dades; control dels processos administratius que els involucren...
- **Transfronterer de forma predeterminada,** facilitant la mobilitat dins el Mercat Únic.
- **Interoperabilitat de forma predeterminada,** lliure circulació de dades i de serveis digitals en la UE.
- **Confiança i seguretat,** més enllà del compliment normatiu de protecció de dades, privacitat i seguretat de TI, integrant aquests elements en la fase de disseny

En aquest sentit, l'Ajuntament de Sant Feliu de Llobregat té un llarg recorregut en el desenvolupament d'accions encaminades al desplegament de l'Administració Electrònica, aprofitant tots els avantatges que les Tecnologies de la Informació i la Comunicació posen a l'abast de les Administracions Públiques, i totes aquelles eines i instruments que la normativa està avalant com a infraestructures fonamentals en aquesta transformació de les organitzacions.

De totes aquestes infraestructures (seu electrònica, carpetes ciutadanes, tauler d'anuncis electrònic, perfil de contractant, registre electrònic, signatura electrònica, expedients electrònics, factura electrònica...), la protecció de dades de caràcter personal és per a l'Ajuntament de Sant Feliu de Llobregat, una peça clau i essencial sobre què pivoten la resta d'instruments i eines necessàries per a la transformació digital de les Administracions Públiques.

2. LA SEGURETAT INTEGRAL

Amb posterioritat, i en desenvolupament de la Llei 11/2007 LAECSP, van ser aprovats els Esquemes Nacionals de Seguretat i Interoperabilitat, regulats pel Reial Decret 3/2010, de 8 de gener i Reial Decret 4/2010, de 8 de gener, el que a la pràctica va requerir que en paral·lel al projecte principal de desplegament de l'Administració Electrònica, l'Ajuntament comencés també a portar a terme totes les accions necessàries per adequar els seus sistemes als preceptes dels esquemes.

En aquest context, el reconeixement del dret a comunicar-se amb les administracions públiques a través de mitjans electrònics comporta una obligació per a aquestes consistent en la promoció de les condicions de seguretat necessàries perquè aquestes transaccions es produeixin en un context adequat de llibertat i igualtat. En aquest sentit cal protegir els actius, sistemes d'informació i dades de les possibles amenaces, al voltant de tres actuacions bàsiques: prevenir, reaccionar i recuperar.

Així, per garantir el compliment de la seguretat dels sistemes d'informació per part de les administracions públiques, la Llei 40/2015 LRJSP, com ja va fer la LAECSP, es va remetre a l'ENS (article 156), aprovat pel Reial Decret 3 / 2010 ENS i que ha estat posteriorment modificat pel Reial Decret 951/2015, de 23 d'octubre.

En concret, l'ENS va venir a instaurar i concebre la seguretat com un procés integral i transversal en l'organització, en un entorn on les TIC impliquen unes noves amenaces per a la seguretat de les transaccions i de les dades, i en especial en relació amb les dades de caràcter personal.

Està constituït pels principis bàsics i els requisits mínims requerits per a una protecció adequada de la informació. Els principis bàsics de l'ENS estableixen uns punts de referència per a la presa de decisions en referència a les mesures de seguretat a prendre. Entre els principis bàsics es troben, com a principis fonamentals: la seguretat com a procés integral; la gestió basada en riscos o el caràcter diferenciat de la seguretat respecte a la gestió de la informació.

En aquell moment es va haver de reformular l'estratègia en matèria de seguretat de la informació per poder atendre els requisits mínims fixats per l'ENS que eren i són d'obligat compliment en el desenvolupament de les polítiques de seguretat que han d'adoptar les Administracions Públiques. Amb l'aplicació d'aquestes mesures de seguretat es pretén, en essència, minimitzar l'impacte que tindrien els incidents de seguretat en els sistemes que permeten la ciutadania exercir drets i complir obligacions.

Cal destacar que en el camí per al compliment de l'ENS va ser necessari realitzar un seguit d'actuacions, per la qual cosa ens va ser de molta utilitat prendre com a punt de partida la planificació que en el seu Portal d'Administració Electrònica, proposa el Ministeri d'Hisenda i Administracions Públiques (a través de diferents guies).

A grans trets, es poden concretar les següents actuacions:

- Preparar i aprovar la política de seguretat de la informació (CCN-STIC 805).
- Realitzar una anàlisi de riscos que inclogui la valoració de les mesures de seguretat existents.
- Preparar i aprovar la Declaració d'Aplicabilitat de les mesures de l'Annex II ENS (CCN-STIC 804).
- Implantar, operativitzar i monitoritzar les mesures de seguretat a través de la gestió continuada de la seguretat corresponent.
- Auditar i verificar la seguretat i el compliment de l'ENS (CCN-STIC 802 i CCN-STIC 808).
- Informar sobre l'estat de la seguretat utilitzant les mètriques i els indicadors definits (CCN-STIC 815 i CCN-STIC 824).
- Elaborar un Pla d'Adequació per a la millora de la seguretat (CCN-STIC 806).

L'adequació a l'ENS té per finalitat l'establiment d'un Sistema de Gestió de la Seguretat de la Informació (SGSI), tal com es recull en l'Annex III ENS, que exigeix la gestió continuada de la seguretat en línia amb els principis bàsics a què s'ha fet referència anteriorment.

En el cas de l'Ajuntament de Sant Feliu de Llobregat, i una vegada aprovat el Pla d'adequació, ens trobem en plena fase de desplegament del Sistema de Gestió de la Seguretat de la Informació, revisant els actius i establint les mesures de seguretat adequades, en base a la recent auditoria realitzada i, també, en base als nous requeriments del RGPD, com es detallarà posteriorment.

3. REORGANITZACIÓ DE LA SEGURETAT A L'AJUNTAMENT

En aquest escenari, una altra de les actuacions de canvi va ser, de manera lògica, una necessària reestructuració de l'organització de la seguretat per garantir el compliment de la normativa tant de protecció de dades de caràcter personal com de seguretat dels sistemes d'informació.

L'organització de la seguretat és un dels elements estratègics per aconseguir implantar un Sistema de Gestió de la Seguretat de la Informació (SGSI) i correspon a cada organització definir a través de la seva política de seguretat el model organitzatiu i detallar les atribucions de cada responsable i els mecanismes de coordinació i de resolució de conflictes. Referent a això, s'ha de tenir en compte que l'ENS estableix la necessària diferenciació entre la responsabilitat de la seguretat dels sistemes d'informació i la prestació dels serveis.

Així, si l'objectiu és tractar la seguretat com un procés transversal i integral, sembla raonable que l'organització de la seguretat es plantegi també des d'una doble perspectiva: la seguretat dels sistemes d'informació i de les dades que es gestionen, és a dir, les responsabilitats derivades del compliment de l'ENS i les derivades del compliment de la normativa sobre protecció de dades personals. A més, cal tenir present que el RGPD estableix també la necessitat d'adoptar mesures de caràcter tècnic, organitzatiu i de seguretat en els processos de tractament de dades.

Existeixen fórmules diverses per a l'organització de la seguretat, encara que a l'Ajuntament de Sant Feliu de Llobregat, es va optar per una organització de la seguretat estructurada en dos òrgans col·legiats, la Comissió i la Subcomissió de Seguretat, que assumeixen funcions en matèria de seguretat de la informació i de protecció de dades de caràcter personal.

Així, finalment, per acord de Junta de Govern Local de 7 de juny de 2011 es va aprovar la reestructuració de l'organització de la seguretat de l'Ajuntament de Sant Feliu de Llobregat, que es va concretar en els següents òrgans col·legiats i unipersonals amb la distribució de competències i funcions:

1. Responsable del fitxer: Ajuntament de Sant Feliu de Llobregat (com a ens públic), representada per la figura de l'alcalde. Les funcions encomanades són les pròpies d'aquesta figura en la normativa en matèria de protecció de dades.

2. Comissió de Seguretat: òrgan col·legiat de caràcter institucional, integrat per membres de l'equip de govern i de l'equip directiu que ostenta funcions de Responsable de la seguretat. Es reuneix com a mínim dos cops a l'any.

3. Subcomissió de seguretat: òrgan col·legiat responsable operatiu, juntament amb l'Oficina d'Atenció Ciutadana. Es reuneix mensualment i està integrat per un tècnic jurídic, el Cap del Departament de RRHH, la Responsable de l'Oficina d'Atenció Ciutadana, el Cap de la Unitat d'Informàtica i la Responsable de la Unitat de Gestió del Coneixement i Qualitat.

4. Dos Administradors de Seguretat: Secretari i Sistemes d'Informació. Són les figures nomenades per la Comissió de Seguretat per tal de fer efectives les mesures de seguretat establertes. Han de vetllar per les funcions de seguretat relacionades amb el Sistema Informàtic i la documentació, la distribució de la Informació a tercers, prèvia autorització per part de la Comissió de Seguretat, i la informació sensible. Els Administradors de Seguretat han d'informar la Comissió de Seguretat amb una periodicitat mensual, i sempre que hi hagi una incidència greu o molt greu de seguretat.

5. Gestors de fitxers: Direccions de serveis, caps de departaments, i caps d'unitat. Són les persones físiques o jurídiques, autoritats públiques, serveis o altres organismes que, sols o conjuntament amb d'altres, tracten dades de caràcter personal autoritzats pel Responsable del Fitxer. Assumeixen a l'Ajuntament les funcions típiques per a aquestes figures.

6. Responsable d'Atenció a l'Afectat: Secretari, juntament amb l'Oficina d'Atenció Ciutadana.

Tant la Comissió de Seguretat com la Subcomissió de Seguretat assumeixen funcions de la LOPD i de l'ENS.

Per tant, el compliment de LOPD, ENS i ENI a l'Ajuntament es porta a terme per la mateixa estructura organitzativa de l'Ajuntament, mitjançant la Comissió i la Subcomissió de Seguretat.

En aquest sentit, vist amb perspectiva, el focus que l'Ajuntament va posar en el desplegament de l'ENS i en la consecució d'un SGSI pot considerar-se un gran encert, perquè com s'ha demostrat, l'evolució de la normativa en matèria de protecció de dades ha evolucionat cap a la consideració de la seguretat en un doble vessant, i en la necessitat d'aplicar mesures de protecció no només a les dades que es tracten sinó també als sistemes d'informació que els suporten. Dóna certa satisfacció observar com el Projecte de la nova LOPD recull com a mesures tècniques a aplicar les establertes a l'ENS, el qual serà necessari que s'adeqüi també a aquesta nova normativa.

Ara queda adaptar aquesta estructura organitzativa en matèria de seguretat als nous preceptes establerts al RGPD per tal de garantir la seguretat de la informació i la protecció de dades, incorporant/adaptant els següents perfils mínims obligatoris:

- Responsable de tractament (RGPD)
- Responsable de la informació (ENS)
- Responsable de seguretat (ENS)
- Delegat/ada de Protecció de dades (RGPD)
- Responsable de Sistemes (ENS)
- Responsable de Servei (ENS i LOPD)

Mantenint l'estructura de la Comissió i de la Subcomissió de Seguretat amb funcions, entre d'altres, de coordinació, control del compliment i establiment de les mesures i els procediments de seguretat establerts a l'Ajuntament.

4. ADEQUACIÓ AL REGLAMENT GENERAL DE PROTECCIÓ DE DADES:

L'adaptació al Reglament General de Protecció de Dades, que serà aplicable a partir del 25 de maig de 2018, requereix de l'elaboració d'una nova llei orgànica que substitueixi l'actual, però mentre es culmina aquest procés, són d'agrair les guies i els materials didàctics que s'han anat publicant per les diferents autoritats de control, la FEMP i per suposat aquesta mateixa guia on es destaquen aquells aspectes de la regulació en el RGPD que impacten de manera directa sobre l'activitat de les administracions públiques, i en especial les entitats locals, com a responsables i encarregades de tractament de dades personals en el desenvolupament de les seves activitats i que ja estem treballant, en el marc de l'organització referenciada, per a la seva consecució.

En aquest sentit, a finals de 2017, en sessió monogràfica conjunta de la Comissió i la Subcomissió de Seguretat, es van posar de manifest les obligacions derivades de l'aplicació del RGPD, per tal de conscienciar tant l'equip de govern com l'equip de direcció de les actuacions que era necessari dur a terme per al compliment normatiu en aquesta matèria.

Les tasques que es van identificar prioritàries abordar durant l'any 2018 per garantir el correcte compliment de l'Ajuntament en l'àmbit de la seguretat de la informació i dades de caràcter personal van ser:

- Adaptació al Reglament General de Protecció de Dades
- Realitzar una auditoria de l'ENS
- Revisió de l'organització de seguretat per encardinar la figura del/de la Delegat/ada de Protecció de Dades

Respecte a l'adaptació al RGPD, algunes de les adequacions en les que ja estem treballant són les següents:

- **Identificar amb precisió les finalitats i la base jurídica dels tractaments i establiment d'un Registre d'Activitats de Tractament.** En aquest sentit, hem sol·licitat a l'Autoritat Catalana de Protecció de Dades còpia del contingut dels fitxers inscrits al Registre de Protecció de Dades de Catalunya, per tal de disposar d'un punt de partida per a l'elaboració del Registre d'Activitats de Tractament. La informació sobre la finalitat i la base jurídica dels tractaments és fonamental per tal de poder establir en quins casos no serà necessari recavar el consentiment de l'afectat. De fet aquest punt és de cabdal importància per complir amb el principi "d'una sola vegada", garantint que la ciutadania i empreses suministren la mateixa informació només una vegada a les AAPP. L'actual article 28 de la LPACAP contempla la pressumpció del consentiment llevat oposició expressa, la qual cosa entra en contradicció amb l'establert al RGPD que prohibeix expressament el consentiment tàcit. Haurem d'esperar si prospera el PLOPD que en la DA 10 estableix la potestat de verificació de les AAPP quan es formulen sol·licituds per mitjans electrònics (esperem que la redacció final no especifiqui només

per mitjans electrònics, ja que és cert que el procediment és únicament electrònic, però la sol·licitud, si no és un subjecte obligat, es pot realitzar presencialment o electrònicament...). En aquest punt és important la interpretació que fa l'AEPD a la recentment publicada *Guia Protecció de Dades i Administració Local*, que en relació amb aquest tema conclou que: "En relación con este precepto, y teniendo en cuenta que el RGPD a efectos de consentimiento no permite el denominado como "tácito", el acceso a los documentos por parte de la Administración pública correspondiente podría fundamentarse en el artículo 6.1.e) del RGPD, es decir, cuando el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, vinculado al hecho de que, de conformidad con la Ley 39/2015, de 1 de octubre, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración.
En este sentido, será suficiente con que la Ley hubiese determinado quién es la Administración competente."

- **Identificar els tractaments gestionats sota el principi de consentiment de l'interessat,** que caldrà que estigui adaptat a les noves exigències del RGPD, és a dir, ha de ser informat, lliure, específic i atorgat pels interessats mitjançant una manifestació on quedi demostrada la voluntat de consentir, o mitjançant una clara acció afirmativa. Com s'ha dit abans, caldrà revisar doncs aquells tractaments on s'hagi utilitzat un consentiment tàcit per tal d'adaptar-ho a la nova normativa, garantint en aquest cas la informació d'aquest canvi a l'afectat perquè pugui exercir els seus drets.

- **Compliment del principi de transparència,** revisant tots els procediments i formularis que tenim a la seu electrònica per tal de garantir el dret d'informació en la recollida de dades personals i l'exercici dels drets dels afectats, donant resposta en els terminis establerts al RGPD. En aquest sentit, hem recollit la recomanació de l'AEPD d'adoptar un model d'informació per capes:

    1. En un primer nivell, al formulari de sol·licitud, presentar la informació bàsica (identificació del responsable, finalitat del tractament, exercici de drets, origen de les dades...), que podrem fer un cop fetes les accions anteriors, ja que necessitem disposar de tota aquesta informació per poder-la oferir a la ciutadania.

    2. En un segon nivell, la informació addicional que implicarà la reformulació de la política de privacitat que actualment tenim publicada al Portal web de l'Ajuntament.

- **Identificar els contractes que impliquin tractament de dades de caràcter personal** per tal d'adequar les clàusules relatives als encarregats de tractament.

- **Estem elaborant també tant la informació dels tràmits com els circuits dels expedients administratius electrònics per tal d'atendre, en temps i forma, els nous drets dels afectats,** el dret d'accés, rectificació, supressió ("dret a l'oblit"), oposició i limitació al seu tractament.

-

- **Elaborar anàlisi de riscos per als drets i llibertats de la ciutadania de tots els tractaments de dades que es desenvolupin, i revisar les mesures de seguretat que s'apliquen als tractament en base a aquesta anàlisi de riscos.** Com s'ha especificat anteriorment en aquest document, l'Ajuntament de Sant Feliu de Llobregat ha organitzat la gestió de la seguretat des d'una perspectiva transversal i, per tant, la recent auditoria de l'ENS ha contemplat tant el compliment dels requeriments establerts en aquesta norma tècnica com també l'adopció de les mesures tècniques i organitzatives que permetin garantir el compliment del RGPD. De fet, com a resultat d'aquesta auditoria s'ha vist la necessitat d'actualitzar els actius de l'Ajuntament i fer una valoració del risc dels tractaments amb l'objectiu de determinar amb més claredat i aplicar les mesures de seguretat que corregeixin o minimitzin els riscos.

- **Elaborar i implementar el procediment d'avaluació d'impacte en la protecció de dades,** en base a la metodologia establerta per les autoritats de control. Aquest és un tema molt important de cara al desplegament real de l'Administració electrònica com un instrument per a la simplificació i la possibilitat d'anticipació dels serveis públics en benefici de la ciutadania. És evident que les AAPP disposem d'una quantitat ingent de dades que ben estructurades poden permetre millorar els serveis públics, passant d'una Administració reactiva (esperant la sol·licitud dels interessats), a una Administració proactiva, per exemple, atorgant subvencions a aquelles persones que compleixen determinats requisits sense necessitat que la ciutadania ho sol·liciti. Però fer això implicaria tractament de dades personals i cal prèviament realitzar aquesta avaluació d'impacte. El mateix pot passar a l'hora de desplegar polítiques d'Smart City, on a més el tractament i l'intercanvi de dades es realitza no només entre AAPP sinó també amb operadors privats.

- **Aprovar la creació del lloc de treball de delegat/ada de Protecció de Dades (DPD), que s'incorporarà a la Comissió i la Subcomissió de Seguretat.** Al Ple de març de 2018, s'ha aprovat el marc estratègic per a la transformació cultural i organitzativa de l'Ajuntament de Sant Feliu de Llobregat que inclou, entre d'altres acords, el desenvolupament d'una estructura organitzativa que incorpori els nous requeriments normatius en matèria de contractació, transparència, control financer, protecció de dades i administració digital, fet que suposa modificar l'organigrama i el catàleg de llocs de treball per, entre d'altres, incorporar el perfil de delegat/ada de protecció de dades de caràcter personal adscrit a la Direcció d'Àrea de Govern Obert i Serveis Generals. Les funcions seran les establertes pel propi RGPD, però també incorporarà altres funcions relacionades amb la reenginyeria de processos, l'administració digital, govern obert, etc, que no siguin incompatibles amb les seves funcions pròpies.

- **Establir els mecanismes per identificar amb rapidesa l'existència de violacions de seguretat de les dades i poder reaccionar davant d'elles.** En aquest cas, l'apli-

cació de les mesures de seguretat estarà marcada pels criteris establerts a l'Esquema Nacional de Seguretat, que s'ha d'adequar també a les previsions del RGPD. Hem d'establir els procediments per comunicar aquestes violacions en els terminis establerts a l'apdCAT, en cas de risc per als drets i llibertats de les persones físiques, i a les persones físiques afectades. A l'Ajuntament de Sant Feliu de Llobregat disposem d'un registre d'incidències, que revisem mensualment a la Subcomissió de Seguretat, per aplicar les mesures tècniques necessàries, i estem elaborant un Pla de contingències que contempli com actuar en cas de caiguda dels sistemes o bé davant d'una bretxa de seguretat.

En aquest sentit, ens hem dotat d'un quadre de comandament per controlar les incidències produïdes en matèria de seguretat:

- **L'adopció del principi de responsabilitat proactiva ("Accountability"),** revisant i mantenint actualitzada permanentment tota la documentació relacionada (Document de Seguretat, Política de Seguretat, Manual de funcions i obligacions, nous procediments...), per tal de poder demostrar en tot moment a qui ho sol·liciti que complim amb el RGPD i que s'han establert els mecanismes i les actuacions necessàries, la qual cosa s'anirà adequant i desplegant progressivament.

- **Formació en matèria de protecció de dades.** L'Ajuntament de Sant Feliu de Llobregat des de fa temps ha incorporat aquesta matèria al seu Pla estratègic de formació i a la Intranet es disposa d'un espai obert per a tots els empleats i empleades públics amb informació permanent, recomanacions, plantilles, presentacions, guies, enllaços d'interès, etc.

5. CONCLUSIONS

De tot el que s'ha exposat, es pot observar amb claredat que l'Ajuntament de Sant Feliu de Llobregat està realitzant un treball de continuïtat en la protecció de les dades de caràcter personal dins de l'organització.

Com exposa molt clarament el Professor Rafael Jiménez Asensio en aquesta Guia, ens trobem davant d'un canvi de paradigma en la concepció de la gestió de la protecció de dades que requereix l'establiment de mesures tècniques però sobretot organitzatives, per tal d'incorporar la seguretat com un procés transversal en l'activitat de les Administracions Públiques. I és raonable que davant el repte de la transformació digital, la seguretat ocupi un paper fonamental per generar la confiança de la ciutadania en l'ús dels mitjans electrònics però també, per garantir la transparència, el retiment de comptes i per suposat els drets i llibertats de les persones respecte a l'ús que fan les Administracions Públiques de les seves dades personals.

L'Administració Digital permet la traçabilitat; controlar els accessos, però es requereix establir les polítiques de seguretat, les mesures organitzatives i els procediments necessaris per tal que, de forma proactiva, es puguin prendre decisions en relació als nous tractaments de la informació i reaccionar ràpidament davant les violacions en matèria de seguretat que es puguin produir.

En aquest sentit, vist amb perspectiva, el focus que l'Ajuntament va posar en el desplegament de l'ENS i en la consecució d'un SGSI pot considerar-se un gran encert, perquè com s'ha demostrat, la normativa en matèria de protecció de dades ha evolucionat cap a la consideració de la seguretat en un doble vessant i en la necessitat d'aplicar mesures de protecció no només a les dades que es tracten sinó també als sistemes d'informació que els suporten.

Sant Feliu de Llobregat, abril de 2018

DOCUMENTACIÓ ANNEXA A LA GUIA

MATERIALS, INFORMES, ARTICLES I RESOLUCIONS SOBRE RGPD

REGLAMENT GENERAL DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL 2016/679

Josep Betriu Sangüesa
Alba Sánchez Hostalot

1. Guies, materials i eines sobre el RGPD i el seu impacte al sector públic

2. Adaptació de la LOPD al RGPD

3. Resolucions de les autoritats de control espanyoles.

4. Anàlisi jurisprudencial sobre Protecció de Dades: Tribunal Suprem, Tribunal Constitucional i Tribunal de Justícia de la Unió Europea.

5. Articles referents a la protecció de dades de caràcter personal.

6. Llibres recentment publicats relacionats amb el Reglament General de Protecció de Dades.

1. GUIES, MATERIALS I EINES SOBRE EL RGPD I EL SEU IMPACTE AL SECTOR PÚBLIC

Reglamento (UE) 2016/679 del parlamento europeo y del consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

GUIES DE LA L'APDCAT

1.1 Guia bàsica de protecció de dades per a ens locals de l'apdCat

Aquesta és una guia elaborada per l'Agència Catalana de Protecció de Dades que, encara que és relativa a la normativa precedent al nou RGPD, pot ser un punt de partida per a certs aspectes que requereixen d'una sèrie d'exigències als responsables dels ens locals.

1.2 Guía sobre cumplimiento del deber de informar según la apdCat

L'objecte d'aquesta guia és orientar sobre les millors pràctiques per complir l'obligació d'informar a les persones interessades, en virtut del principi de transparència, sobre les circumstàncies i les condicions del tractament de dades a efectuar, així com dels drets que les assisteixen. Igual que en altres guies, trobarem una part introductòria en la qual, una vegada superada, trobarem eines útils.

1.3 Guia pràctica - Avaluació d'impacte relativa a la protecció de dades

Des de l'apdCat es va redactar aquesta guia que serà útil per poder realitzar una avaluació d'impacte amb garanties. En aquesta guia s'explicaran quins són els aspectes preparatoris, l'anàlisi de la necessitat de realitzar una avaluació d'impacte, la descripció sistemàtica de les operacions de tractament, i finalment disposarem de models que poder aplicar.

1.4 Guia sobre l'encarregat del tractament en el Reglament General de Protecció de Dades (RGPD)

La guia elaborada per l'Autoritat Catalana de Protecció de Dades en col·laboració amb l'Agència Espanyola de Protecció de Dades i l'Agència Basca de Protecció de Dades, persegueix identificar els punts clau a tenir en compte al moment d'establir la relació entre el responsable del tractament i l'encarregat del tractament, així com identificar les qüestions que afecten de manera directa la gestió de la relació entre els dos.

GUIES DE L' AEPD

1.5 Guía sobre Reglamento General de Protección de Datos para responsables de tratamiento de la AEPD

Aquesta guia resumeix les novetats del Reglament Europeu i els canvis que hauran de tenir en compte els responsables de les organitzacions que tractin dades de caràcter personal ja siguin privades o públiques. Conté, fins i tot, un llistat de verificació de caràcter simplificat que podria ser d'ajuda per a aquelles entitats locals amb un nombre de ciutadans menor.

1.6 Guía sectorial de la AEPD sobre Protección de Datos y Administración Local

La guia tracta aquells aspectes del Reglament que afecten l'Administració Local i compte, al seu torn, amb un catàleg de preguntes freqüents relatives al RGPD i al tractament de dades de caràcter personal realitzat per aquests ens públics.

1.7 Directrices para la elaboración de contratos entre responsables y encargados de tratamient

Aquestes directrius són una guia elaborada, de forma conjunta, per les autoritats de protecció de dades existents a Espanya. Hi trobarem els processos adequats per elaborar un contracte amb totes les garanties per als implicats, així com adaptar-se a totes les exigències del RGPD.

1.8 Guía de anonimización de la AEPD

Aquesta guia està realitzada per donar suport per al cas que les entitats públiques, o privades, requereixin publicar una sèrie de dades amb finalitats d'estudi o estadístics i es garanteixin l'anonimat dels subjectes objectes de l'estudi.

1.9 Decálogo para la adecuación al Reglamento General de Protección de Datos en las Administraciones Públicas.

Aquest conte una numeració de les regles bàsiques del RGPD que afecten els organismes públics.

1.10 Guía para la adaptación del Reglamento General de Protección de Datos, de las Administraciones Locales, FEMP, Grupo de Trabajo para la Implantación del nuevo RGPD en las Administraciones Locales.

Aquesta és una guia molt recent i molt actualitzada on l'AEPD i la FEMP han tractat sobre el RGPD des d'una perspectiva local.

1.11 Listado de cumplimiento normativo para la adaptación del RGPD

Aquest llistat ha estat editat el passat 13 d'abril per l'AEPD i és un mètode bàsic que permet obtenir una visió general del grau d'adequació d'un tractament de dades personals al RGPD, sent especialment útil tant per als processos d'analisi de risc com en les avaluacions d'impacte.

GUIES DEL GRUP DE TREBALL DE L'ARTICLE 29

1.12 Grup de Treball de l'article 29

Els treballs del Grup, creat per la Directiva Europea 95/46, tot i que no són jurídicament vinculants, tenen un important valor doctrinal i són freqüentment utilitzats i citats pels legisladors i els tribunals nacionals i europeus, es així que hem de referenciar alguns d'aquests com a eines molt útils per entendre i aplicar la nova normativa sobre protecció de dades.

- ***"Guidelines on Personal data breach notification under Regulation 2016/679"*** Sobre bretxes als sistemes de seguretat dels tractaments i com actuar d'avants d'aquestes segons la normativa Europea.
- ***"Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/67".*** Sobre com realitzar perfils individuals:

detalla els drets dels usuaris i diferencia dades de caràcter especial o que pertanyen a subjectes sensibles a fi de realitzar tractaments més acurats.

- ***"Data Protection Officers".*** Sobre la importantíssima figura de l'encarregat de protecció de dades: realitza un estudi rigorós respecte a l'encarregat i les seves tasques a realitzar.
- ***"Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk"* for the purposes of Regulation 2016/679".** Aquesta guia és essencial per entendre què és l'avaluació d'impacte i per identificar el risc dels diferents tractaments.
- ***"Guidelines on the right to data portability"*** Sobre les directrius del dret a la portabilitat, que el Reglament ha atorgat als usuaris de tractaments de dades personals.
- ***"Dictamen del Grupo de Trabajo del Artículo 29 sobre el tratamiento de datos en el*** ámbito ***laboral"***. Directrius sobre l'avaluació d'impacte relativa a la protecció de dades (EIPD) i per determinar si el tractament «comporta probablement un alt risc» a l'efecte del Reglament (UE) 2016/679.

Tots els treballs i dictaments estan accessibles a la direcció web: http://collections.internetmemory.org/haeu/20171122154227/http:/ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

MATERIALS DELS ÒRGANS EUROPEUS

1.13 Comunicació de la Comissió al Parlament Europeu, al Consell, al Comitè Econòmic i Social Europeu i al Comitè de les Regions.

Igual que la tecnologia, la forma en què les nostres dades personals s'utilitzen i comparteixen en la nostra societat està en evolució constant. És en virtut d'aquest avenç inexorable, l'any 2010, la Comissió entén que és essencial adaptar-se al mateix, i amb l'objectiu d'actualitzar i unificar el règim, aquesta presenta una iniciativa de projecte de reglament. Aquest document serà la base del posterior en aquest moment, i actual RGPD.

1.14 Orientacions de la Comisió Europea sobre l'aplicació directa del Reglament General de Protecció de Dades.

La Comissió Europea realitza aquest comunicat, el contingut del qual són una sèrie de pautes, pretén donar una idea de la necessitat d'adaptar-se el més aviat possible al RGPD ja que, com s'expressa en el comunicat, la nova norma és d'aplicabilitat directa. En el mateix comunicat trobarem els objectius per a les properes fases.

1.15 Propuesta de Reglamento del Parlamento Europeo y del consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos).

Aquesta proposta és el text que precedeix i assenta les bases de l'actual Reglament General de Protecció de Dades. Útil per a aquells que tinguin un interès especial en l'evolució de la nova regulació.

1.16 *A Statementon Artificial Intelligence, Robotics and 'autonomous' systems by the European Group of Ethics and Science in New Technologies.*

Aquest document de 9 d'abril de 2018, ens permet plantejar-nos la posició de la protecció de dades a l'Europa de la intel·ligència artificial.

REAL DECRETO NACIONAL COMPLEMENTARIO A LA NORMATIVA DE PROTECCIÓN DE DATOS

1.17 Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

2. ADAPTACIÓ DE LA LOPD AL RGPD

2.1 Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal

Amb l'objectiu d'adaptar-se al RGPD, el Congrés dels Diputats, amb l'assessorament de l'AEPD, va redactar el projecte de llei que, àdhuc per aprovar, s'albira la seva aplicació a partir dels mesos finals de 2018.

2.2 Informe de la AEPD sobre el Anteproyecto de la LOPD

El Gabinet Jurídic de l'Agència Espanyola de Protecció de Dades va emetre el següent informe en la seva funció preceptiva virtut de l'anterior llei LOPD. En el mateix informe l'AEPD donarà la seva opinió sobre una llei en la qual ella mateixa ha intervingut de forma intensa.

2.3 Dictamen del Consejo de Estado sobre el anteproyecto de la LOPD

En aquest text el Consell d'Estat mirarà de proposar solucions a aquelles qüestions que puguin erigir-se com a dubtoses o fora dels principis constitucionals o que, en tot cas, vagin en contra de les disposicions normatives de rang europeu

2.4 Informe del Consejo Fiscal al Anteproyecto de Ley Orgánica de protección de datos de carácter personal.

Conforme als principis de col·laboració entre òrgans constitucionals, han de ser expressades les consideracions del Ministeri Fiscal sobre aspectes que afectin drets i llibertats fonamentals.

3. RESOLUCIONS DE LES AUTORITATS DE CONTROL ESPANYOLES.

3.1 Agencia Española de Protección de Datos

Procedimient de Declaració d'Infracció contra Consorcio de Emergencias de Gran Canaria.

La captació d'imatges a través de càmeres constitueix un tractament de dades personals on el responsable de les mateixes és qui decideix sobre la finalitat, contingut i ús del tractament. Aquest ha d'assegurar que no es captin imatges de persones a la via pública ni de l'espai d'intimitat de treballadors i, en tot cas, ha d' avisar de l' ús de videovigilància per motius del 20.3 ET.

Procedimient sancionador de l'AEPD contra la Conselleria de Sanitat Universal de la Generalitat Valenciana.

Si els centres sanitaris per actes o omissions revelen, entre d'altres, el nom i el document nacional d'identitat dels pacients, es considera una vulneració al principi de seguretat, consagrat en la LOPD i la directiva europea, i en l'obligació de guardar el secret professional.

L'AEPD no imposa cap sanció econòmica degut a què la LOPD no preveu sancions econòmiques a les Administracions Públiques.

3.2 Autoritat Catalana de Protecció de Dades

Informe emès a petició de la Comissió de Garantia del Dret d'Accés a la Informació. Accés a informació del padró municipal d'habitants.

La normativa de protecció de dades no impedeix la comunicació d'informació de l'empadronament a l'hereu d'una persona morta, encara que aquestes dades afectin terceres persones, sinó sembla que la comunicació d'informació comportí un perjudici significatiu pel dret d'aquestes i a més hi ha un interès directe d 'accés a la informació pública per part del solicitant.

Dictamen en relació a la transferència internacional de dades personals d'entitats de dret públic.

Deixant de banda les comunicacions de dades destinades a països de la UE, així com aquelles efectuades a Argentina i Israel, les transferències preteses per l'entitat només es podran efectuar si s'aporten garanties adequades sobre la protecció que les dades rebran a la seva destinació en els termes establerts a l'article 46 de l'RGPD. Si els destinataris no ofereixen un nivell adequat de protecció i no s'apliquen les excepcions de l'article 49.1 de l'RGPD, la cessió vulnera la protecció de dades.

3.3 Agencia Vasca de Protección de Datos

Dictamen relatiu a la cesión de dades a serveis socials per diferents ens locals.

No existeix cessió de dades quan els ens locals demanen que se'ls torni dades que varen facilitar als serveis socials si la informació sol·licitada coincideixi amb l'aportada per aquelles. En cas contrari, es requerirà consentiment o habilitació legal, a no ser que la informació personal fos estrictament necessària per a l'exercici de les competències de l'Administració sol·licitant, cas en què legalment es permet la cessió de dades entre administracions.

Dictamen sobre la cessió de dades d'empleats públics (domicili i número de telèfon) a la Tesorería General de la Seguridad Social.

Tot i que es permet la comunicació de dades entre Administracions Públiques sense consentiment dels interessats, no és aplicable quan la comunicació no es realitza per a l'exercici de competències idèntiques ni versen sobre les mateixes matèries. En aquest cas, la sol·licitud del número de telèfon mòbil d' empleats públics requereix el consentiment de l'interessat, tot i que l'Administració consultada, de conformitat amb el principi de col·laboració entre Administracions Públiques, podria informar als empleats públics afectats que la TGSS requereix aquelles dades.

4. ANÁLISI JURISPRUDENCIAL SOBRE PROTECCIÓ DE DADES: TRIBUNAL SUPREM, TRIBUNAL CONSTITUCIONAL I TRIBUNAL DE JUSTÍCIA DE LA UNIÓ EUROPEA.

4.1 Tribunal de Justícia de la Unió Europea.

Assumpte "X" C-486/12 de 12 de desembre de 2013. **El dret de l'administració a rebre una contrapartida per l'exercici del dret d'accés a les dades personals,** permès pel dret europeu i fixat lliurement pels Estats membres, no podrà excedir l'import del cost de la comunicació d'aquestes dades a l'usuari que les demani.

Assumpte Google Spain C-131/12 de 3 de mayo de 2014. L'activitat d'un motor de cerca ha de considerar-se un tractament de dades quan conté dades de caràcter personal**, el gestor d'un motor de cerca ha de considerar-se responsable d'aquest tractament** i **el dret a l'oblit l'obliga a eliminar de la llista de resultats aquella cerca a partir del nom d'un usuari** tot i que aquesta informació sigui lícita en si mateixa.

Assumpte Digital Rights Ireland Ltd C293/12 y C594/12 de 8 d'abril de 2014. La conservació de dades per prestadors de serveis per temps extensos quan constitueixin mesures necessàries i proporcionades per a finalitats específiques d'ordre públic, com protegir la seguretat nacional sobrepassa els límits que exigeix el respecte del principi de proporcionalitat en relació amb el dret al respecte a la vida privada i a la llibertat d'expressió de la Carta de Drets Humans.

Assumpte Minister voor Immigratie, Integratie en Asiel C-141/12 y C-372/12, de 17 de juliol de 2014. **El dret d'accés de l'usuari que tramita una sol·licitud administrativa**, respecte totes les seves dades personals que siguin objecte del tractament, comporta que se l'ha de facilitar una idea completa d'aquestes dades en forma intel·ligible, permetent-li conèixer-les i comprovar que són exactes i

tractades de conformitat amb el dret europeu a fi que pugui, si s'escau, exercir els drets pertinents.

Assumpte František Ryneš C-212/13 de 11 de diciembre de 2014. La utilització d'un sistema de càmera de vídeo, que dóna lloc a l'obtenció d'imatges de persones que després s'emmagatzemen en un dispositiu d'enregistrament continuat, com un sistema de videovigilància instal·lat per una persona física en el seu habitatge familiar amb la finalitat de protegir els béns, la salut i la vida dels propietaris de l'habitatge i la vigilància del qual cobreix també l'espai públic, no constitueix un tractament de dades efectuat en l'exercici d'activitats exclusivament personals o domèstiques a l'efecte de la Directiva 95/46/CE.

4.2 Tribunal Constitucional

Auto 29/2008 de 28 de gener. La protecció de dades professionals i salarials, aquestes tenen caràcter personal com *"totes aquelles que identifiquin o permetin la identificació de la persona, podent servir per a la confecció del seu perfil[...] o que serveixin per a qualsevol altra utilitat que en determinades circumstàncies constitueixi una amenaça"* implica que els òrgans públics tenen obligació de denegar qualsevol sol·licitud d'aquelles quan no sigui proporcionada, no ho autoritzi una llei o no respongui a una necessitat justificada.

Sentència 17/2013 de 31 de gener. **La licitud de cessió interadministrativa de dades quan així ho permet una llei,** la Llei Orgànica de drets i llibertats dels estrangers preveu aquesta cessió si existint un determinat expedient és necessària la informació especifica que obra en mans d'un altre òrgan de l'Administració Pública i per tant, si no es tracta d'una transmissió massiva o indiscriminada de dades.

Sentència 29/2013 de 11 de febrer. La facultat de saber en tot moment qui disposa de les dades personals i amb quina finalitat, és un *"element característic de la definició constitucional de l'art. 18.4 CE, del seu nucli essencial"*. És un dret d'informació de l'usuari que opera, fins i tot, quan hi ha una exigència legal per recavar informació de caràcter personal sense consentiment d'aquell.

4.3 Tribunal Suprem

Sentència 545/2015 de 15 d'octubre. **El dret a l'oblit**: **La caducitat de l'acció al dret a l'oblit** s'inicia quan el perjudicat coneix el fi del tractament ja que els danys que derivin d'aquest es consideren danys continuats en el temps. L'exercici d'aquest dret també s'aplica **als tractaments de dades per hemeroteques digitals** doncs van "*perdent la seva justificació a mesura que transcorre el temps si les persones concernides manquen de rellevància pública i els fets, vinculats a aquestes persones, manquen d'interès històric"***.**

Sentència 1455/1960 de 20 de juny de 2016. **El contingut dret a l'oblit comporta: Un deure** del responsable a *"adoptar totes les mesures raonables"* per suprimir o rectificar dades que o bé no responen a períodes necessaris i a fins específic o bé no són exactes, necessàries i actualitzades i**, a la vegada, un dret** de l'usuari a oposar-se al seu tractament. Es considerarà **responsable tot aquell que col·labori en un tractament** quan la seva activitat sigui ***"indispensable per al funcionament"*** d'aquest.

Sentència 1749/2016 de 13 de Juliol de 2016. **L'administració i el dret a requerir certes dades a entitats privades,** l'article 11.1 LOPD 15/1999 permet que es puguin transferir dades a tercers quan una llei així ho autoritzi i per tant, una sol·licitud per part de l'Administració Tributària d'informació amb finalitats fiscals no és un acte lesiu.

Sentència 2423/2016 de 14 de Novembre. **Una ponderació entre els drets de protecció de dades i els dret a la llibertat d'expressió i informació,** implica observar l'especial protecció que mereixen les llibertats d'expressió i d'informació sobre la resta de drets fonamentals que *"es projecta també sobre el dret a la protecció de dades de caràcter personal"* -tot i que això- *"no significa que en tots els casos de conflicte hagi de predominar".*

5. ARTICLES REFERENTS A LA PROTECCIÓ DE DADES DE CARÀCTER PERSONAL.

5.1 Rafael Jiménez Asensio. "Algunas reflexiones sobre la figura del Delegado de Protección de Datos en las Administraciones Públicas"

Publicació: Revista L'Administració al Dia.
Estudis i comentaris. 18 de Gener de 2018.

Resum: Falta poc per a la plena aplicabilitat del Reglament (UE) 2016/679 i aquest article tracta la pretensió d'aquesta entrada i emmarca el problema centrant-se sobretot en la figura del Delegat de Protecció de Dades. L'article analitza l'estatut jurídic del Delegat de Protecció de Dades; el nivell orgànic que hauria de tenir i com s'haurien de cobrir aquests singulars llocs de treball, assenyalant, amb tot, els nous reptes de les administracions públiques.

5.2 Enrique Rubio Torrano. "Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal"

Publicació: Revista Doctrinal Aranzadi Civil-Mercantil num.1/2018 parte Legislación.
Editorial Aranzadi, S.A.U., Cizur Menor. 2018.

Resum: "El 10 de novembre de 2017, el Consell de Ministres va aprovar el Projecte de Llei Orgànica de Protecció de Dades de Caràcter Personal, una vegada procedit el tràmit d'enviament al Consell d'Estat, que va dur a terme les corresponents observacions al text presentat i que, al fil d'aquestes, va experimentar algunes modificacions. El text va a ser sotmès al corresponent procediment legislatiu després del seu ingrés al Congrés dels Diputats (Butlletí Oficial de les Corts Generals. Congrés dels Diputats, 24 de novembre de 2017). El comentari que segueix enquadra la nova Llei Orgànica en el marc normatiu i jurisprudencial europeu i espanyol."

5.3 Miguel Ángel Ácero. "España es una referencia en la legislación sobre la protección de datos"

Publicació: Vlex
Id.Lex:VLEX-554490454

Resum: Miguel Ángel Acer és expert en innovació i tecnologia de TIC Centre Tecnològic, i expert en e-commerce (comerç electrònic) i seguretat digital entre altres matèries, totes relacionades a les noves tecnologies de la informació i la comunicació. En el present analitza la situació actual de l'ús de la xarxa i les seves conseqüències. "Quan utilitzem les xarxes socials facilitem informació sobre nosaltres i autoritzem les grans corporacions al fet que la usin".

5.4 Lucia Salvador Alamar. "La protección de datos"

Publicació: Vlex
Id.Lex: VLEX-695713969

Resum: Dos anys passen volant. S'aproxima el termini de dos anys concedit pel Reglament Europeu de Protecció de Dades [Reglament (UE) 201 6/679] a totes les empreses o organitzacions establertes en la Unió Europea, públiques o privades, que recaptin o tractin dades personals de persones físiques en el desenvolupament de la seva activitat per adaptar-se a aquesta nova normativa, que serà de plena aplicació a partir del 25 de maig de 2018.

5.5 Ana Isabel Herrán Ortiz. "Aproximación al derecho a la protección de datos personales en Europa. El reglamento general de protección de datos personales a debate"

Publicació: R.E.D.S.núm.8,Enero-Julio2016
ISSN:2340-4647

Resum: Recentment es publicava l'esperat Reglament General de Protecció de Dades a la Unió Europea. Molt temps s'ha hagut d'esperar fins a l' aprovació d'aquesta norma i moltes han estat les expectatives jurídiques que aquest text havia generat. Pretenem en aquest treball presentar unes breus notes que analitzin algunes de les novetats més significatives d'aquest Reglament, que si bé no serà aplicable fins a 2018, exigirà, com tindrem ocasió d'explicar, un gran esforç dels Estats membres per adaptar el seu dret nacional al nou context legal europeu en protecció de dades personals.

5.6 Concepción Campos Acuña, "Los 7 imprescindibles en protección de datos para el ámbito local", El Consultor de los Ayuntamientos y Juzgados, enero 2018

Publicació: LA LEY *828/2018*

Resum: En el present article, examinem els 7 imprescindibles a tenir en compte per les Entitats Locals per donar compliment a les previsions recollides en el Reglament Europeu de Protecció de Dades, aplicable a partir d'una data propera: 25 de maig de 2018

5.7 Noticia sobre la reprimenda de la AEPD al creador d'un grup de WhatsApp il·legal

Publicació: Vlex
Id.Lex:VLEX-694748717

Resum: L'Agència de Protecció de Dades amonesta a un restaurant mallorquí per elavorar un llistat amb les dades dels clients que van reservar una taula.

6. LLIBRES RECENTMENT PUBLICATS RELACIONATS AMB EL REGLAMENT GENERAL DE PROTECCIÓ DE DADES.

1. Reglamento General de Protección de Datos

Jose Luis Piñar Aragoneses, 2016. Editorial Reus.

Ressenya de l'editor: "Aquest llibre és la primera obra col·lectiva a Espanya, i segurament a Europa, sobre el nou Reglament Europeu de Protecció de Dades. En ell es desgranen les principals novetats que incorpora la nova normativa, que serà plenament aplicable a partir de maig de 2018. [...] Incorpora, entre altres qüestions, nous principis com el privacy by default, privacy by design o el principi de responsabilitat proactiva (accountability); drets nous com el dret a l'oblit o el dret a la portabilitat; regula i impulsa la figura del Delegat de Protecció de Dades (DPO), important novetat per al nostre país."

2. Claves prácticas para la protección de datos: Protección de Datos Personales: adaptaciones necesarias al nuevo Reglamento europeo

Luis Felipe López Álvarez, 2017. Editorial Francis Lefebvre.

Ressenya de l'editor: "[...]Aquesta nova monografia de la col·lecció Claus Pràctiques resulta imprescindible pels qui exerceixin el lloc de Delegat de Protecció de Dades, però també per startups, serveis de cloud computing, empreses, advocats, professionals, Administracions Públiques i, en general, per a qualsevol que, d'una forma o una altra, estigui afectat per la normativa de protecció de dades [...] En resum, un manual de marcat caràcter pràctic, que exposa el que hi ha i el que ve, un text de fàcil consulta indispensable per a qui hagi de gestionar el dia a dia de la protecció de dades de caràcter personal."

3. Practicum Protección de Datos 2018

Javier. Álvarez Hernando, 2017. Editorial Aranzadi.

Resenya de l'editor: "Estudi dels assumptes més rellevants en matèria de protecció de dades personals des d'una perspectiva jurídica, d'una forma senzilla i estructurada, incloent, els fitxers de morositat; videovigilància; tractaments de dades d'advocats i procuradors; comunitats de propietaris, centres de salut, Administració Pública i centres de formació. [...]."

4. Nuevo Reglamento Europeo de Protección de Datos Versus Big Data

Faustino Gudín Rodríguez Magariños, 2018. Editorial Tirant lo Blanch

Ressenya de l'editor: "[...]No és aquests el cas, perquè les regulacions han estat tan aclamades com a necessàries com el nou Reglament. Amb aquesta norma, d'aplicació directa i prevalent per a tots els ciutadans de la Unió, Europa s'erigeix en una potència mundial un marc de referència mundial i, a l'una, es postula com potser la societat democràtica més avançada. En conseqüència, conèixer i saber utilitzar aquesta importantíssima normativa se'ns intueix un haver de jurista com una necessitat ciutadana.

No obstant això, aquest capital instrument normatiu només pot ser apropiadament comprès i calibrat, dins del complex patrimoni normatiu i jurisprudencial que li confereix el seu veritable sentit."

5. El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos

José López Calvo, 2018. Editorial Bosch.

Ressenya de l'editor: "[...] La present obra, coordinada per José López Calvo, realitza un examen exhaustiu del seu text, així com del projecte de llei de Protecció de Dades de Caràcter Personal que va aprovar el Consell de Ministres el 10 de novembre de 2017. De la mateixa manera, i gràcies a la participació d'un equip d'autors de reconegut prestigi i provada solvència, s'incorpora la perspectiva i el criteri de les principals institucions, sectors i operadors implicats que analitzen la transcendència sectorial del nou marc regulatori. Finalment, l'obra es completa amb aportacions eminentment pràctiques que traslladen experiències concretes per facilitar la implantació del nou marc."

6. Una revisión del derecho fundamental a la protección de datos de carácter personal

Mónica Martínez López Sáez, 2018. Editorial Tirant lo Blanch

Ressenya de l'editor: "[...] El present estudi ha procurat analitzar la situació actual i els avenços recents, a nivell normatiu i jurisprudencial, per modelar i reforçar el dret fonamental a la protecció de dades de caràcter personal, com a resposta a l'imparable progrés tecnològic-digital. Es pretén, per tant, identificar, d'una banda, els diferents sistemes de protecció, així com les sinergies i llacunes jurídiques existents en l'àmbit del dret de la protecció de dades en la Unió Europea i el Consell d'Europa, i per un altre, donar resposta als reptes als quals s'enfronta per a l'establiment d'un sistema de protecció efectiva."