COL·LEGI DE SECRETARIS, INTERVENTORS I TRESORERS D´ADMINISTRACIO LOCAL DE LLEIDA

EL NOU REGLAMENT 2016/679

DE PROTECCIO DE DADES PERSONALS

INDEX

1.- LES NOTICIES DELS MITJANS DE COMUNICACIÓ

- Robat d'un ambulatori un ordinador amb dades confidencials de 15.000 malalts.
- Protecció de dades inicia la investigació de Sánchez Romero per l'escàndol dels currículums.
- Subhasten a ebay un ordinador amb milions de dades bancàries.
- L'APD multa amb 180 milions de pessetes a Zeppelin per la fuga de dades d'aspirants a "gran hermano".
- Multa de protecció de dades per un 'e-mail' no desitjat.
- 500 analítiques localitzades en la brossa.
- Google haurà d'oblidar el teu passat.
- Condemnat un metge a 3 anys de presó per accedir a l'historial d'un company.

2.- EXEMPLES D'INFRACCIONS D´ADMINISTRACIONS PÚBLIQUES (APDCAT)

- L'emmagatzematge de contrasenyes dels usuaris de forma intel·ligible als sistemes d'informació suposa una infracció del principi de seguretat. Concorren els requisits per a la rebaixa d'un grau en la imposició de la sanció, i en aplicació del principi de proporcionalitat s'imposa una multa de 32.000 euros.
- El fet que un Ajuntament possibiliti que determinades persones -el personal de l'empresa que controla la zona blava del municipi i el personal de l'Associació de Voluntaris de Protecció Civil- accedeixin a totes les dades de caràcter personal tractades pels membres la Policia Local en les converses mantingudes a través de dispositius walkie-talkie, fet propiciat per la compartició de la freqüència de ràdio, és una infracció del principi de seguretat.
- El SOC va vulnerar el deure de secret quan envià, per error, dades personals a una tercera persona referents a la revocació d'un ajut.
- El Grup municipal ha comès dues infraccions greus per haver difós per internet a través del seu bloc diverses sessions del Ple municipal que contenien dades personals, sense l'autorització de l'alcalde, i sense el consentiment de les persones afectades ni habilitació legal, ni la creació del corresponent fitxer.

- La recollida de dades de persones implicades en danys a béns municipals a través d'impresos que no contenen la clàusula informativa de tots els extrems de l'art. 5 LOPD constitueix una infracció lleu.

- La implantació d'un sistema de videovigilància amb enregistrament d'imatges i veus sense la prèvia creació del fitxer mitjançant disposició general, constitueix una infracció greu. Així mateix, la captació d'imatges de persones a la via pública és constitutiva d'una infracció greu, al considerar-se excessiva en relació a les finalitats perseguides. No informar degudament de l'existència de les càmeres és constitutiu d'una infracció lleu.

- L'encarregat de tractament en la gestió d'enviaments d'avisos de pagament d'impostos, va produir un error massiu (en l'elaboració dels enviaments, de tal manera que en el revers de les comunicacions enviades a milers de destinataris, hi figurava informació referent a d'altres contribuents, vulnerant d'aquesta manera el deure de secret de les dades.

- S'adverteix a l'AMPA per la comissió d'una infracció lleu al haver tractat dades personals dels seus associats sense haver sol·licitat la inscripció de fitxer en el Registre de Protecció de Dades.

- El lliurament d'un certificat que conté dades relatives a la salut a una persona diferent del seu titular, sense comptar amb el consentiment exprés d'aquest, és constitutiu d'una infracció molt greu.

3.- EXEMPLES D'INFRACCIONS D'EMPRESES

- Vulneració del deure de secret mitjançant trucades a familiars per el recobrament de deutes.

- Difusió a web especialitzada d'una sentència sense anonimitzar amb dades sensibles.

- Difusió per un gimnàs d'un fitxer amb dades de 9.293 persones adjunt a un correu electrònic. Vulneració del deure de secret.

- Publicació de comunicat mèdic d'incapacitat d'una treballadora al perfil de facebook de la seva empresa.

- Concurs de TV remet de forma massiva SMS no sol·licitats i sense mitjà d'oposició.

- Difusió a Internet del cens de treballadors per un sindicat.

- Recollida de dades de menors sense consentiment patern a lloc web.

- Documentació d'hospital a contenidor de brossa.
- Càmera sense cartell informatiu per controlar treballadors.
- Correu electrònic amb adreça en obert de múltiples destinataris.
- Documents en via pública d'acadèmia de policia.
- Tractament a facebook d'imatge de tercers.
- Sanció per crear un perfil fals de tercer en xarxa social.
- Codi d'usuari i contrasenya genèrica que permeten accés indiscriminat.
- Enviament sense còpia oculta de dades de deute a 129 afectats.
- Càmera de centre comercial enfocant via pública.
- Ús d'imatge de menor en cartell publicitari.
- Comunitat de propietaris difon imatges per Internet.
- Dades clínica dentista a EMULE.

4.- LES PRINCIPALS NOVETATS

4.1.- La tramitació del RGPD

- Procés llarg: De 2009 a 2016
- Aprovació: 27-4-2016
- Publicació DOUE: 4-5-2016
- Entrada vigor: 25-5-2016
- Aplicable 25-5-2018
- Norma complexa
    - 173 considerants
    - 99 articles

4.2.- Les raons

- Directiva 95/46 adaptada de maneres diverses per països UE
    - Cas espanya amb interès legítim
- Entorn digital
- Seguretat jurídica

- Harmonització complerta

4.3.- Enllaços d'interès

EUROPA

- http://ec.europa.eu/justice/smedataprotect/index_es.htm?utm_content=buffera534f&utm_medium=social&utm_source=linkedin.com&utm_campaign=buffer#mobile-menu

- https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/reform/rules-business-and-organisations_es

ESPANYA

- https://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php

CATALUNYA

- http://apdcat.gencat.cat/ca/documentacio/RGPD/

4.4.- El concepte més important: La Responsabilitat activa (accountability)

- Es una transformació del model formalista actual (declarar fitxers, tenir documents de seguretat, etc) al govern responsable de les dades

- Els responsables i les encarregats aplicaran:
  - les mesures tècniques i organitzatives apropiades
  - per garantir
    - les obligacions
    - per estar en condicions de demostrar-ho

- Aquestes mesures es revisaran i actualitzar quan sigui necessari

- La no aplicació d'aquestes mesures és sancionable

- Tipus de mesures aplicables que acrediten la responsabilitat activa:

  - Mantenir Registre d'activitats de tractament
  - Aplicar mesures de seguretat adequades
  - Mesures de Protecció de Dades des del Disseny
  - Mesures de Protecció de Dades per defecte
  - Dur a terme Avaluacions d'Impacte
  - Designació Delegat Protecció de Dades (DPO)
  - Notificació dels incidents de Seguretat

- Aprovar codis de conducta i esquemes de certificació
- Formar al personal

4.5.- la convivència de la LOPD i Reglament Europeu

- Fins al 24-5-2018
    - la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (LOPD)
    - el seu Reglament de desplegament (RLOPD), aprovat pel Reial decret 1720/2007, de 21 de desembre, continuen essent de plena aplicació.

- A partir del 25-5-2018
    - alguns aspectes de l'LOPD i de l'RLOPD quedaran desplaçats per l'RGPD.

- El projecte de llei de reforma de la lopd
    - http://www.mjusticia.gob.es/cs/Satellite/Portal/1292428594682?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=attachment%3B+filename%3DPLOPD_TEXTO_APROBADO_CM_10-11-2017.PDF
- Difícilment hi haurà nova LOPD abans del 24-5-2018

- Es una reglament directament aplicable, per tant es la norma de referencia

- L'RGPD va entrar en vigor el 24 maig de 2016 i serà de plena aplicació a partir del 25 de maig de 2018.

- Durant aquest període de dos anys, els responsables i encarregats de tractaments han d'adequat les operacions de tractament que duen a terme al que preveu l'RGPD, adoptant les mesures necessàries per atendre adequadament les modificacions que introdueix el Reglament i, en especial, els nous principis, els nous drets i les noves obligacions que preveu

4.6.- Àmbit d'aplicació

- Subjectiu
    - persones físiques identificables
        - concepte pseudonimitzacio.
    - tractament automatitzat i no automatitzat (excepcions)
        - apostasia
    - Exclusió

        - persona domestica exercici activitats exclusivament personals o domestiques
        - Cas Lindqvist
        - Xarxes socials i persones físiques?
            - El administrador de una pàgina de fans de una red social como Facebook es un responsable del tratamiento.
                - http://curia.europa.eu/juris/document/document.jsf?text=&docid=195902&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=934990
        - Vigilancia al carrer
            - Instalación de cámaras en vehículos privados: El tratamiento de imágenes de personas en vía pública corresponde a las fuerzas y cuerpos de seguridad, sin que pueda incluirse en principio dentro de la excepción doméstica la utilización de cámaras con intención de grabar infracciones penales o administrativas cometidas en vía pública.
                - http://www.avpd.euskadi.eus/documentacion/-/dictamen_avpd/d16_040/
- Territorial
    - El Reglament s´aplica a RT i ET establerts dins UE
        - Ja existia
    - Amplia l'àmbit d'aplicació territorial als responsables i els encarregats del tractament no establerts a la UE, quan
        - les activitats de tractament estan relacionades amb l'oferta de béns o servei
            - us moneda, llengua destinatari, etc
        - amb el control del comportament de les persones, si tenen lloc a la UE.
    - Aplicació dret internacional

4.7.- Categories especials de dades

- Categories especials de dades, dues noves categories especials de dades:
    - Suposa disposar de DPO (art. 37 RGPD)
    - Dades genètiques:
        - dades personals relatives a les característiques genètiques heretades o adquirides d'una persona física que proporcionen una informació única sobre la fisiologia o la salut d'aquella persona, obtingudes en particular de l'anàlisi d'una mostra biològica.
    - Dades biomètriques:
        - dades personals obtingudes a partir d'un tractament tècnic específic, relatives a les característiques físiques, fisiològiques o conductuals d'una persona física que permeten o confirmen la identificació única d'aquesta persona
            - imatges facials,
            - dades dactiloscòpiques,
            - etc.

- Prohibició de tractament llevat
    - Art. 9 RGPD (consentiment explícit, obligacions dret laboral, seguretat i protecció social, protecció interès vital dades publiques, interès públic essencial i medicina preventiva?

4.8.- Consentiment

- Es una de les bases per legitimar el tractament es el consentiment

- Es una manifestació lliure, inequívoca, especifica i informada a traves de la qual l´interessat consenteix el tractament de les seves dades

- Es ok

    - el consentiment mitjançant una declaració inequívoca
    - o una acció afirmativa clara.

- No es Ok
    - Les caselles ja marcades,
    - el consentiment tàcit
    - o la inacció no constitueixen un consentiment vàlid.

- Molt rellevant en les comunicacions comercials per via electrònica i el procediment de l´article 19 del reglament 1720/2007

4.9.- Consentiment dels menors

- En l'àmbit dels serveis de la societat de la informació el consentiment dels menors
    - S´estableix una forquilla entre 16 i 13
    - Per tant els estats membres de la UE poden rebaixar l'edat fins als 13 anys.
        - El que serà aplicable aquí
    - A més, el llenguatge emprat per informar-los els ha de ser comprensible.

4.10.- El dret d'informació

- Amplia les qüestions sobre les quals cal informar-les:
    - les dades de contacte del delegat de protecció de dades;
        - obligatori a totes les Administracions Publiques
    - la base jurídica del tractament
        - la legitimació segons l´article 6 del RGPD
    - els interessos legítims perseguits en què es fonamenta el tractament, si escau;

- la intenció de transferir les dades a un país tercer o a una organització internacional i la base per fer-ho, si escau;
    - important conèixer on s´allotjen les dades
- el termini durant el qual es conservaran les dades;
- el dret a demanar la portabilitat;
- el dret a retirar en qualsevol moment el consentiment que s'ha prestat;
- si la comunicació de dades és un requisit legal o contractual o un requisit necessari per subscriure un contracte;
- el dret a presentar una reclamació davant d'una autoritat de control;
- l'existència de decisions automatitzades, inclosa la lògica aplicada i les seves conseqüències.

4.11.- Drets dels interessats

- El dret a l´oblit
    - Novetat?
        - Tema AEPD / google stjce 13-5-2014
        - Dret oposició
        - https://support.google.com/legal/contact/lr_eudpa?product=websearch
    - Les persones interessades tenen dret a obtenir la supressió de les dades ("dret a l'oblit"), quan:
        - Les dades ja no són necessàries per a la finalitat per a la qual es van recollir.
        - Es revoca el consentiment en el qual es basava el tractament.
        - L'interessat s'oposa al tractament.
        - Les dades s'han tractat il·lícitament.
        - Les dades s'han de suprimir per complir una obligació legal.
        - Les dades s'han obtingut en relació amb l'oferta de serveis de la societat de la informació adreçats a menors.
    - Quan el responsable ha fet públiques les dades personals i s'hagin de suprimir, ha d'adoptar mesures raonables per informar de la supressió els responsables que estan tractant les dades.
    - Es preveuen algunes excepcions a l'exercici d'aquest dret:
        - L'exercici del dret a la llibertat d'expressió i d'informació.
        - El compliment d'una obligació legal.
        - L'existència de finalitats d'arxiu en interès públic, d'investigació científica o històrica o finalitats estadístiques.
        - La formulació, l'exercici o la defensa de reclamacions.

- Dret a la portabilitat
    - La persona interessada té dret a rebre les dades personals que l'afecten que hagi facilitat a un responsable del tractament en un format estructurat, d'ús comú i de lectura mecànica, i a transmetre-les a un altre responsable, si es compleixen els requisits següents:
        - El tractament està basat en el consentiment o en un contracte
        - El tractament es fa per mitjans automatitzats

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

- Dret a la limitació del tractament

4.12.- Inscripció i notificació de fitxers, ara es diu RAT (registre d´activitats de tractament)

- Es suprimeix, a partir del 25 de maig de 2018
    - la necessitat de crear formalment els fitxers
    - i notificar-los al registre de protecció de dades de les autoritats de control

- Ara tindrem el registre d´activitats de tractament
    - Possiblement caldrà publicar-lo al web

- Obligacions de documentació del tractament per als responsables o els encarregats del tractament que compleixen alguna de les condicions següents:
    - Tenen 250 treballadors o més.
    - Tenen menys de 250 treballadors, però duen a terme un tractament que:
        - Pot comportar un risc, no ocasional, pels drets i llibertats de les persones interessades.
        - Inclou categories especials de dades.
        - Inclou dades relatives a condemnes o infraccions penals
    - Aquests responsables i encarregats del tractament han de portar un registre de les activitats de tractament que duen a terme que ha de contenir, respecte cada activitat, la informació que estableix l'article 30 de l'RGPD.

4.13.- Encarregats del tractament

- Son encarregats de tractament les empreses que presten serveis de
    - Gestoria o consultoria que realitza les nòmines, la comptabilitat, l´assessoria jurídica, etc
    - Informàtica (hosting, housing).
    - Seguretat i/o videovigilància.
    - Digitalització, custòdia i de destrucció de paper i de suports informàtics.
    - Neteja.
    - Control d'accés (empremta dactilar o altres mitjans).
    - Recobrament de deutes.
    - Administradors de finques.
    - Impressió d'etiquetes i/o distribució de correspondència i enviaments postals.
    - Tele-màrqueting, d'enquestes de satisfacció al client, etc.
    - Concessionaris
        - Aigua
        - Zona blava
        - Grua

- El Reglament amplia el contingut mínim del contracte d'encarregat de tractament i sobretot cal ser diligent a l´hora de triar-lo
    - l'objecte i la durada de l'encàrrec;
    - la naturalesa del tractament;
    - el tipus de dades personals;
    - les categories d'interessats;
    - les obligacions i els drets del responsable;
    - la previsió que les persones que han de tractar les dades s'han compromès a mantenir la confidencialitat
    - l'assistència de l'encarregat al responsable perquè pugui atendre les sol·licituds d'exercici de drets;
    - la supressió o la devolució de les dades en finalitzar l'encàrrec;
    - l'obligació de posar a disposició del responsable tota la informació necessària per demostrar que compleix les obligacions de l'encarregat del tractament i per permetre i contribuir a la realització d'auditories i inspeccions per part del responsable o d'un altre auditor autoritzat pel responsable.

4.14.- Mesures de seguretat: l´analisi de riscos

- el Reglament
    - no estableix un llistat de les mesures de seguretat que són d'aplicació d'acord amb la tipologia de dades objecte de tractament,
    - sinó que estableix que el responsable i l'encarregat del tractament han d'aplicar mesures tècniques i organitzatives adequades al risc que comporta el tractament.
- Això implica haver de fer una avaluació dels riscos que comporta cada tractament, per determinar les mesures de seguretat que cal implementar.
- Quin procediment apliquem?
    - Esquema nacional de Seguretat
- La guia de l´Agpd
    - https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/AnalisisDeRiesgosRGPD.pdf

4.15.- Notificació de violacions de seguretat

- Si es produeix una violació de la seguretat
    - el responsable ha de notificar-ho a l'autoritat de control en un termini màxim de 72 hores, llevat que sigui improbable que constitueixi un risc per als drets i les llibertats de les persones
    - A més, quan sigui probable que la violació comporti un alt risc per als drets de les persones interessades, el responsable els l'ha de comunicar sense dilacions indegudes i en llenguatge clar i senzill, tret que:

- El responsable hagués adoptat mesures de protecció adequades, com ara que les dades no siguin intel·ligibles per a persones no autoritzades
- Hagi aplicat mesures posteriors que garanteixen que ja no hi ha la probabilitat que es concreti l'alt risc
- Suposi un esforç desproporcionat.

4.16.- Avaluacions d'impacte relatives a la protecció de dades (PIA – privacy impact assessment)

- Es una nova obligació del RGPD:
  - avaluar l'impacte de les operacions de tractament en la protecció de les dades personals, quan sigui probable que el tractament comporti un risc significatiu per als drets i les llibertats de les persones

- AGPD: Guia para una evaluación de impacto en la protección de datos personales
  - https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_EvaluacionesImpacto.pdf

- APDCAT: guía practica. Avaluació d´impacte relativa a la protecció de dades
  - http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/GUIA-AIPD-APDCAT.pdf

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

- Privacy by design
  - Això implica que cal que el responsable aplicarà, tant en el moment de determinar els mitjans de tractament com en el moment del tractament mateix, les mesures tècniques i organitzatives adequades (com per exemple la seudonimització), concebudes per aplicar de manera efectiva els principis de protecció de dades, i integrar les garanties necessàries en el tractament, per complir els requeriments del Reglament.

- Privacy by default:
  - Així mateix, el responsable ha d'aplicar les mesures tècniques i organitzatives adients per garantir que, per defecte, només es tracten les dades personals necessàries per a cada finalitat específica del tractament.

4.18.- Delegat de protecció de dades (DPO)

- Introdueix la figura del delegat de protecció de dades

    - pot formar part de la plantilla del responsable o de l'encarregat
    - o actuar en el marc d'un contracte de serveis.

- Cal designar un delegat de protecció de dades en els casos següents:
    - Quan el tractament l'efectua una autoritat o un organisme públic (tret de jutjats i tribunals).
        - En aquest cas, es pot designar un únic delegat de protecció de dades per a diverses d'aquestes autoritats o organismes.
    - Quan el tractament requereix l'observació habitual i sistemàtica d'interessats a gran escala.
    - Quan el tractament té per objecte categories especials de dades personals o dades relatives a condemnes o infraccions penals.

- El delegat de protecció de dades té, entre d'altres, les funcions següents:
    - Informar i assessorar el responsable o l'encarregat i els treballadors sobre les obligacions que imposa la normativa de protecció de dades.
    - Supervisar el compliment de la normativa
    - Assessorar respecte de l'avaluació d'impacte relativa a la protecció de dades.
    - Cooperar amb l'autoritat de control.
    - Actuar com a punt de contacte per a qüestions relatives al tractament.

- Qui pot ser DOP
    - APEP
        - http://www.apep.es/tag/dpo/
    - Model de notificació APDCAT

https://seu.apd.cat/es/tramits/DPD

4.19.- Transferències internacionals

- Algunes modificacions en aquest àmbit,
    - com ara el reconeixement exprés de les normes corporatives vinculants com a base per a la transferència de dades dins un grup empresarial.
        - https://www.agpd.es/portalwebAGPD/jornadas/7_sesion_anual/common/JPH_TID_GARANTIAS_NORMAS_CORPORATIVAS_VINCULANTES_7SAA.pdf

- En vigor privacy shield
    - http://europa.eu/rapid/press-release_IP-16-2461_es.htm

4.20.- Codis de conducta

- L'RGPD també regula els codis de conducta que poden promoure les associacions i altres organismes representatius de categories de responsables del tractament o encarregats del tractament per a la correcta aplicació del Reglament.
- El codi de conducta s'ha de presentar a l'autoritat de control competent per a que l'aprovi el registri i el publiqui.
- També correspon a l'autoritat de control acreditar l'organisme de supervisió previst en el codi.
- L'adhesió i el compliment d'un codi de conducta és un element a tenir en compte a l'hora de demostrar que el responsable del tractament compleix les obligacions, en especial, en el moment de fer l'avaluació d'impacte sobre la protecció de dades.

4.21.- Mecanismes de certificació

- El Reglament també promou els mecanismes de certificació, com ara certificats, segells o marques, com a mecanisme per demostrar que es compleix l'RGPD.
    - Segell europeu de protecció de dades

4.22.- Finestreta única

- Aquest sistema permet que els ciutadans i també els responsables establerts en diferents estats membres o que efectuïn tractaments que afecten diferents estats membres tinguin una única autoritat de protecció de dades com a interlocutora.

4.23.- Sancions

Sancions 10.000.000 / 20.000.000 euros o si es empresa 2 0 4 % com màxim volum negoci total anuals

5.- COM ADAPTAR-SE

Sector públic

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/Adaptacion_RGPD_AAPP.pdf

Sector privat

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/Adaptacion_RGPD_sector_privado.pdf

5.1.- La reunió inicial

- En la reunió inicial es concretaran tasques, prioritzant en tot cas totes aquelles accions en funció dels majors riscos que afrontin o resolguin
    - Presentació dels equips i els seus interlocutors. S'ha de permetre participar en el procés i fer aportacions a tots els afectats pel mateix, tant departaments de l'organització com a socis o entitats externes, afectats o altres agents socials, per exemple
        - Representant amb capacitat de decisió
        - El DPD
        - El responsable de seguretat
- Definició del full de ruta, el calendari i les etapes.
- Planificació de les entrevistes.
- Definició de l'estàndard de seguretat aplicable
- Organigrama dels departaments en que s´organitzen els clients
    - Fluxe de tractaments

5.2.- El Registre d'Activitats de Tractament (art. 30)

- Es tracta d'identificar i inventariar tots els tractaments de dades de caràcter personal que es realitzen:
    - tant quan actuen com a responsables del tractament
    - com quan actuen com a encarregats del tractament,

- Però nomes obligatori per a organitzacions de mes de 250 treballadors
    - llevat tractament incorpori riscos drets i llibertat
    - o sigui ocasional
    - o tracti categories especials de dades o dades relatives a condemnes i infraccions penals

- Cal partir dels tractaments registrats a l´Agència o Autoritat Espanyola de Protecció de Dades
- Un sistema que funciona es els fluxos d'informació (cicle de vida de les dades):
    - recollida,
    - circulació,
    - cessions,
    - recepció de dades d´altres organitzacions,
    - destrucció de les dades,

- El resultat d´aquest procés es
    - la creació del registre d'activitats de tractament.
        - https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles
    - El diagrama del flux de cadascun dels tractaments de dades personals.

5.3.- Designar el delegat de protecció de dades (arts. 37 a 39):

- Es determinarà l'obligació de designar un delegat de protecció de dades tenint en compte el conjunt de tractaments del client i per tant cal preparar la següent documentació:
    - El document de la designació formal (sigui personal intern o extern);
    - La descripció del catàleg de funcions;
    - Notificar la designació a l´Autoritat de Protecció de Dades competent.

5.4. Avaluació d´impacte (art. 35)

- El RGPD incorpora una nova obligació pels responsables de tractaments:

    - avaluar l'impacte que els tractaments de dades personals poden tenir sobre la protecció de les dades quan l'ús de tecnologies avançades, o el volum de dades tractades, o el tipus de dades (categories especials), puguin posar en risc els drets i llibertats de les persones
    - En primer lloc cal fer una anàlisi de si el tractament encaixa dintre dels supòsits per als quals el RGPD preveu aquesta avaluació d'impacte i, si és així, s'ha de procedir a aplicar un mètode d'avaluació que compleixi amb els requisits previstos al RGPD, en aquest sentit s'utilitzarà el mètode proposat a la guia d'avaluació d'impacte de l'APDCAT.

- Quan s´ha de fer (AGPD)
    - Enriquir informació existent o be us amb diferents finalitat
    - Tractament de dades de menors
    - Tractaments adreçats a avaluar o predir el comportament dels afectats
    - Grans volums de dades (big data), internet de les coses (internet of things) o ciutats intel·ligents (smart cities)

- Tecnologies especialment invasives com la vigilància a gran escala, mineria de dades, biometria, tècniques genètiques, ecolocalització, rfid
- Tractament afecti a nombre elevat de persones o s´acumulen gran quantitat de dades dels afectats
- Cessió de dades amb tercers
- Transferència de dades a països que no formen part del EEE i que no tinguin un nivell adequat de protecció
- Us de formes de contacte amb persones especialment intrusives
- Us de dades no dissociades o anonimitzades de manera irreversible amb finalitats estadístiques, històriques o d'investigació científica
- Tractament sistemàtic i massiu de dades especialment protegides
- Existència de riscos específics de seguretat que puguin comprometre la confidencialitat, integritat o disponibilitat de les dades

- Qui esta obligat?
  - Només el responsable del tractament (amb el suport de l´encarregat i del DPD)

- Quin és el contingut mínim?
  - Es regula a l´article 35.7 del RGPD

- Cal publicar-la?
  - No es obligatori, però es pot fer per generar confiança i per aplicació del principi de transparència
  - La documentació ha d´estar a disposició de les autoritats de supervisió

- El DPD i les EIPD
  - Quan el responsable del tractament ha de dur a terme una AIPD ha de buscar l'assessorament del delegat de protecció de dades.
  - Aquest suport el podem entendre tant com una intervenció activa en el disseny i execució de l'avaluació, amb funcions de coordinació o d'interlocució principal amb els avaluadors, o bé de col·laboració amb l'avaluador, si resulta que no ha d'assumir un paper principal en l'AIPD.
  - Quan l'RGPD descriu les funcions que, com a mínim, ha de desenvolupar el delegat de protecció de dades, fa referencia també a la supervisió que necessàriament ha d'exercir respecte de la correcta aplicació del resultat de l'avaluació; és a dir, la verificació que tant l'execució de l'AIPD com la implantació de les mesures (decisions) resultants de l'AIPD son adequades.

- Que passa si no es fa o es realitza de manera no adequada?
  - Exposem els tractaments a riscos no detectats, no s´han adoptat les mesures adequades amb efectes als drets i llibertats de les persones, el que suposa riscs d´infraccions

- Una vegada feta l´EIPD, hi continua el riscs?
  - Fer una consulta prèvia abans d´iniciar el tractament a l´autoritat de supervisió, facilitant informació + te 8 setmanes per contestar per escrit (ampliable)

- La revisió de l´EIPD
    - El tractaments poden variar en el temps, que poden afectar als riscos i per tant cal revisar l´eipd quan es produeixen canvis rellevants

- Els documents que cal generar son:
    - Informe sobre la necessitat o conveniència de fer l'avaluació d'impacte;
    - L'avaluació d´impacte sobre la protecció de dades personals
    - En el seu cas, es gestionarà la consulta prèvia a l'Autoritat de Protecció de Dades competent

- Bibliografia:
    - grup art. 29
        - https://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/common/Traduc_oficial_ult_version/wp248_rev.01_es.pdf
    - Guia AGPD
        - https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
    - Guia APDCAT
        - http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/GUIA-EVALUACION-DE-IMPACTO-CAST.pdf

5.5.- Política de protecció de dades personals

- El RGPD preveu que, quan resulti proporcional als tractaments que realitza el responsable, aquest apliqui polítiques de protecció de dades

- Un exemple de política:
    - https://www.ehu.eus/documents/1870470/3758157/Reglamento+UPV+proteccion+de+datos+libro.pdf/2b08a74c-a871-4208-9ee9-cf09f88d0c44

5.6.- Gestió dels riscos (art. 24.1)

- Un dels elements més rellevants de la nova regulació és que totes les decisions relacionades amb les operacions de tractament, no només les relacionades amb la seguretat de les dades, s'han de prendre d'acord amb la gestió de risc i, addicionalment, s'incorpora el principi de responsabilitat proactiva.

- El que implica el principi de responsabilitat proactiva és la necessitat d'adoptar les mesures orientades al compliment de manera que es pugui demostrar que, efectivament, han estat implantades i que compleixen amb les previsions i requisits del RGPD.

- S´aplica l´esquema nacional de seguretat

    - http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_12_12-ides-idphp.php

- Per tant, en aquesta etapa, es defineixen les mesures tècniques i organitzatives que han de garantir el compliment del RGPD (art. 24 i 25), abordant qüestions com:

    - **Licitud del tractament (art. 6 a 10): quina base jurídica legitima el tractament?**
        - consentiment (explícit o inequívoc, prohibició consentiment tàcit o x silenci, cal establir nous procediments per demanar-lo per les comunicacions comercials per via electrònica)
        - relació contractual
        - interès vital
        - obligació legal per al responsable
        - interès públic o exercici de poders públics
        - interès legítim
        - categories especials de dades personals (art. 9)
        - tractaments sense identificació (art. 10)
    - **Informació i transparència (art. 12 a 14): clàusules informatives segons els requisits del RGPD i les recomanacions de les autoritats de protecció de dades:**
        - Guia de la AGPD sobre el dret d'informació:
            - https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf
        - la obligació d´informar es del responsable
        - es por informar al moment de captar les dades o després
        - llenguatge senzill i clar
        - revisar formularis en paper i electrònics, contractes
        - Informació per capes, es a dir informació bàsica + informació addicional

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

- Un exemple d'informació bàsica

Información básica sobre Protección de Datos	
Responsable	Ediciones Warren&Brandeis, S.A.
Finalidad	Gestión de la suscripción
Legitimación	Ejecución de un contrato
Destinatarios	No se cederán datos a terceros, salvo obligación legal
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web: http://www.warrenbrandeis.com/protecciondatos

- **Drets de les persones interessades (art. 15 a 22);**
  - accés, rectificació, cancel·lació i oposició
  - nous drets:
    - dret a l´oblit,
    - a la portabilitat
    - a la limitació del tractament

- **Encarregat de tractaments (elecció i contractació, art. 28 i 29);**
  - La guía de l´AGPD: Directrius per la elaboració de contractes entre responsables i encarregats
    - https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricescontratos.pdf
  - Elements a considerar:
    - han de tenir un registre d´activitats de tractament
    - determinar les mesures de seguretat
    - designar un DPD en els casos necessari
    - els responsables nomes poden contractar encarregats que ofereixin suficients garanties
    - formalitzar contracte per escrit
    - adaptar-se abans del 25-5-2018

- **Formació i instruccions al personal (art. 29);**

- **Transferències internacionals (art. 44 a 49), si s'escau;**

  - privacy shield
    - http://europa.eu/rapid/press-release_IP-16-2461_es.htm
  - Important conèixer allotjament dels servidors: Guía cloud aGPD:
    - https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf

- **Certificació (art. 42 i 43)**
    - En aquest moment no aplica, ja que encara no existeixen les certificacions o segells de compliment que preveu el RGPD;

- **Seguretat de les dades (art. 32)**
    - Descripció documental de les mesures de seguretat a implantar, sense selecció de tecnologies, ni especificacions tècniques
    - anàlisi de risc (a diferencia de les mesures de seguretat del rd 1720/2007, capítol viii)
    - fer EIPD (PIA) en els supòsits regulats
    - mesures de responsabilitat activa en funció del ris
    - després de l'anàlisi de risc, es determinen les mesures de seguretat aplicables, moltes d´elles seran les mateixes que ja tenim o de vegades caldrà complementar-les
    - privacy by design i by default (abans d´iniciar el tractament)

- **Gestió d'incidències (art. 33 i 34)**
    - Procediments de notificació i comunicacions de violacions de la seguretat de les dades segons el que preveu el RGPD;
        - suposa la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d´una altra forma o la comunicació no autoritza a les dades
        - per exemple la pèrdua d´un portàtil, o l´esborrat accidental de dades personals
        - quan es produeix, obligació de comunicació a l´autoritat en 72 h i si ha suposat la violació de seguretat un alt risc per als drets i llibertats dels interessats, notificació als interessats
        - model per operadors de serveis de comunicacions electròniques
            - https://sedeagpd.gob.es/sede-electronica-web/vistas/formQuiebraSeguridad/procedimientoQuiebraSeguridad.jsf

- **Protocol d'actuació davant de situacions de potencials infractors:**
    - Canals de denúncies internes;
    - Inspeccions;
    - Expedients sancionadors;

- **La implantació**
    - La implantació material de les diferents mesures com les clàusules informatives, contractuals, procediments, normatives internes, etc
    - Els entregables son:

- Clàusules
- contracte d´encarregat de tractament
- exercici i resposta als drets dels afectats
- política de protecció de dades

5-7.- Auditoria o verificació compliment RGPD (art. 24.1)

Gràcies !

Ramon Arnó Torrades, advocat

ramon@sagaris.cat

- https://www.facebook.com/ramon.arno.torrades
- http://es.linkedin.com/in/ramonarnotorrades/

- http://www.sagaris.cat/
- http://www.lafamiliadigital.es/
- http://iusfranquicias.es/
- http://www.caragol.cat/
- http://www.larocasobirana.cat/
- http://www.elmuseodeinternet.es/