Nova Llei de Protecció de Dades europea, què canvia?

Ja ha entrat en vigor el Reglament europeu de protecció de dades, i serà aplicable obligatòriament als dos anys de la seva entrada en vigor, es a dir, el **25 de maig de 2018**.

Aquest Reglament pretén donar **major poder als interessats** sobre les seves dades personals, tant en xarxes socials, smartphones, banca online, etc., de manera que tindran un major control sobre les seves dades.

A continuació tens un **resum dels principals canvis** i que impliquen per el dia a dia

¿Quines empreses estaran obligades a complir amb el RGPD?

Aquest Reglament s'aplica a totes aquelles **entitats** que tractin dades de carácter personal que es trobin dins de la Unió Europea.

També s'aplicarà als **responsables i encarregats** no establerts a la UE sempre que tractin dades com a conseqüència d'una oferta de bens o serveis destinats a **ciutadans de la Unió.**

Noves obligacions

Aquest Reglament suposa un major compromís de les empreses i organitzacions amb la Protecció de Dades.

Rendició de comptes

S'amplia la informació que s'ha de donar als interessats en relació amb el tractament de les seves dades així com als seus drets en aquesta matèria..

S'incorpora el concepte de **privacitat des de el disseny**, de tal manera que es tradueix en que l'elaboració dels procediments empresarials s'ha de realitzar tenint en compte la protecció de les dades des de un primer moment.

Notificació de violacions de seguretat

La nova normativa exigeix que las **violacions en la seguretat** que puguin afectar a les dades personals siguin notificades en un màxim de **72 hores** a la Autoritat de Control corresponent "***Agencia Española de Protección de Datos***".

Si a més en aquest violació es poden veure afectades dades de caràcter sensible i amb una gran repercussió als afectats, també se'ls hi 'haurà de notificar a ells.

Registre de les activitats del tractament

La nova normativa, elimina la obligació de registrar els fitxers en l'autoritat de Control corresponent. (AEPD)

No obstant obliga a portar un registre intern de tots els tractaments de les dades personals que porta l'entitat, sempre que aquesta tingui **més de 250 empleats** o quant es tractin, no de forma ocasional, **dades sensibles**.

Amb menys de 250 treballadors

Sempre serà obligatori, independentment del número de treballadors, si el tractament de les següents dades:

- Que existeixi un risc per els drets i llibertats dels interessats
- Siguin relatives a condemnes i infraccions penals
- de manera no ocasional, inclou categories especials de dades personals (indicades en l'article 9 del RGPD)
    - origen ètnic o racial
    - opinions polítiques
    - conviccions religioses o filosòfiques
    - afiliació sindical
    - tractament de dades genètiques
    - dades biomètriques dirigides a identificar de manera unívoca a una persona física (empremtes dactilars, reconeixement facial)
    - dades relatives a la salut o dades relatives a la vida sexual o las orientacions sexuals de una persona física

Contingut

El RGPD diferencia el contingut depenen de si el Registre el fa el Responsable del fitxer o el Encarregat del tractament.

Registre del Responsable del fitxer

Ha de contenir:

- identificació i dades de contacte del responsable, co-responsable, representant i delegat de protecció de dades
- finalitat del tractament
- descripció de les categories dels interessats i les seves dades
- categories dels destinataris existents o previstos (inclòs en tercers països i organitzacions internacionals)

- transferències Internacionals de dades i documentació de garanties per transferències de dades internacionals exceptuant les realitzades sobre bases d'interessos legítims imperiosos

No obstant, quant sigui possible s'haurà afegir el següent contingut:

- terminis previstos per la supressió de les dades.
- descripció general de les mesures de seguretat:
  a. pseudonimització i xifrat de les dades personals.
  b. capacitat de garantir la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes i serveis de tractament.
  c. restaurar la disponibilitat i l'accés a les dades personals de forma ràpida en caso de incident físic o tècnic.
  d. procés de verificació, avaluació y valoració regulars de la eficàcia de les mesures tècniques i organitzatives per garantir la seguretat del tractament.

Registre del Encarregat del tractament

El registre que ha de portar l'encarregat ha de contenir la següent informació:

- identificació i dades de contacte del encarregat, de cada responsable per compte de qui actua, del representant del encarregat o del responsable, y del Delegat de Protecció de Dades
- las categories de los tractaments efectuats per compte del responsable
- transferències internacionals de dades i documentació de garanties per transferències de dades internacionals exceptuant les realitzades sobre base de interessos legítims imperiosos
- quant sigui possible, una descripció general de les mesures de seguretat

¿Cóm mantenir aquest registre?

Els responsables y los encarregats del tractament (que estigui obligats) hauran de mantenir els registres de les activitats de tractament **sempre actualitzats** que es trobin sota la seva responsabilitat.

Ambdós estan obligats a cooperar amb l'autoritat de control, a España la AEPD, i a posar a la seva disposició, prèvia sol·licitud, els registres de manera que puguin servir per supervisar les operacions del tractament.

Format

Aquest registre haurà de constar sempre **en format electrònic** encara que també es considera vàlid que consti per escrit.

El Delegat de Protecció de Dades - DPO

Una de les principals novetats que implica el Reglament és la creació de la figura del Delegat de Protecció de Dades (***data protection officer***).

El **DPO**, és en gran mesura, la persona encarregada d'informar a la entitat responsable o al seu encarregat del tractament sobre les seves obligacions legals en matèria de protecció de dades.

També haurà de vetllar o supervisar el compliment normatiu així como de cooperar amb l'autoritat de control i actuar com un punt de contacte entre aquesta i l'entitat responsable del tractament de les dades.

La nova normativa fa al **DPO** una figura molt important per l'empresa.

En conseqüència, per el bon desenvolupament de les seves funcions se l'haurà de dotar dels recursos necessaris per portar els seu treball amb plenes garanties i la suficient estabilitat.

Cal destacar també que les seves **dades de contacte hauran de ser públiques**, per que els interessats y supervisors puguin contactar amb ell de manera directa i confidencial.

Funcions del DPO

Els principals **objectius del Delegat de Protecció de Dades** son:

Assessorament

- Ha d'informar i assessorar al responsable o al encarregat del tractament de les obligacions normatives en protecció de dades que els incumbeixin.
- Té que assessorar tant al responsable com al encarregat de l'avaluació d'impacte que faci relativa a la protecció de dades.
- Assessorar als treballadors durant el tractament de les dades.

Supervisió del compliment normatiu

- Supervisar el adequat compliment de les normes sobre protecció de dades en l'entitat.
- Revisar las polítiques internes de privacitat en la organització i la seva adequació normativa.
- Assignar responsabilitats entre los membres de la organització, respecte a les obligacions en matèria de protecció de dades.

- Realització de accions de conscienciació internes respecte al compliment efectiu de la normativa.
- Formar al personal que participa en las operacions de tractament de dades.
- Supervisar les avaluacions d'impacte en la protecció de dades.
- Control, coordinació i verificació de les mesures de seguretat aplicables.

Cooperació i enllaç amb l'autoritat de control

- Actuar como punt de contacte amb la *Agencia Española de Protección de Datos* per a les qüestions relacionades amb el tractament de les dades personals, inclosa la consulta prèvia.
- Cooperar con la autoritat de control.

Atenció als interessats

- Atendre les consultes que facin els interessats a l'entitat, ja sigui per qüestions relatives al tractament de les seves dades o per el exercici dels seus drets.

Obligatorietat de comptar amb un DPO

No sempre es necessària la figura d'un delegat de protecció de dades en la nostra organització.

obligatorietat de la seva designació en estos casos:

1. Quan el tractament de les dades sigui realitzat por una autoritat o un organisme públic.
2. Si les activitats principals del responsable o del encarregat consisteixen en operacions de tractament que, en raó de la seva naturalesa, arribi a finalitats que requereixin una observació habitual i sistemàtica d'interessats a gran escala.
3. Si las activitats principals del responsable impliquen el tractament a gran escala de dades especials o personals referides a condemnes o delictes.

Entitats en que és obligatori la designació de un DPO:

Col·legis professionals

Centres docents

Prestadores de serveis de comunicacions electròniques

Aquí s'inclouen les **companyies telefòniques** i els proveïdors d'accés a Internet, sempre que tractin perfils a gran escala.

Prestadores de serveis de la societat de la informació

En aquest cas estaríem parlant d'una botiga "*online*", una xarxa social, etc, quan **s'elaboren perfils a gran escala** dels usuaris del servei.

Entitats de Crèdit

Entitats de crèdit com bancs, les caixes d'estalvis, les cooperatives de crèdit i el Instituto de Crédito Oficial.

Empreses de foment de la finançament empresarial

Entitats asseguradores

Empreses de serveis d'inversió

Les que ofereixen **serveis d'inversió en la borsa i** de fons d'estalvi.

Distribuïdores i comercialitzadores d'electricitat

Les companyies elèctriques, i també les entitats que venen al públic electricitat.

Organitzacions que avaluen la solvència patrimonial i crèdit

S'inclouen els responsables dels fitxers regulats per la Llei de prevenció del blanqueig de capitals i de la finançament del terrorisme.

Empreses de publicitat i prospecció comercial

S'inclouen aquelles empreses que es dediquen al *marketing* elaborant perfils del consumidor.

Centres sanitaris

Diversos tipus de centres sanitaris, como hospitals, clíniques estètiques o clíniques dentals, les quals estan obligats a mantenir la historia clínica del pacient.

Emissores de informes comercials

Empreses on la seva activitat principal es la aportació d'informes relatius al comerç realitzat per persones físiques.

Operadors de joc electrònic

Entitats que ofereixen apostes esportives *online*, així como també jocs de casino.

Empreses de seguretat privada

Les que realitzen les activitats regulades per el Títol II de la Llei 5/2014, de 4 de abril, de Seguretat Privada. S'inclouen també les empreses que proporcionen seguretat privada així com també els despatxos de detectius privats.

Canvis en els drets ARCO de Protecció de Dades

S'introdueixen nous elements, que augmenten la **capacitat de decisió i control** dels ciutadans sobre les dades personals que faciliten a tercers.

Dret al oblit

Es el dret que tenen els ciutadans a sol·licitar, i aconseguir dels encarregats, que les dades personals siguin suprimides quan aquestes ja no siguin necessàries per la finalitat per la que es varen obtenir, quan s'hagi revocat el consentiment o quan aquestes s'hagin obtingut de forma il·legal.

Dret a la portabilitat

Implica que el interessat que hagi proporcionat les seves dades a un responsable que els estigui tractant de forma digitalitzada podrà requerir recuperar aquestes dades en un format que li permeti el seu trasllat a un altre responsable.

Canvis en la obtenció del consentiment

El Reglament demana que el consentiment, amb caràcter general, sigui **lliure, informat, específic i inequívoc**.

Las empreses **hauran de revisar** la forma en la que obtenen i guarden el consentiment.

Actualment existien pràctiques que s'enquadren en el consentiment tàcit i que son acceptades amb l'actual normativa però **deixaran de ser-ho** quan el Reglament sigui d'aplicació.

Per poder considerar que el consentiment es "inqüestionable", el Reglament requereix que hi hagi una declaració dels interessats o una **acció positiva** que apunti al acord del interessat.

La acceptació no es podrà deduir del silenci o de la inacció dels ciutadans.

S'exigeix que el consentiment tingui de ser **"manifest"** en determinats casos, como pot ser per **autoritzar el tractament de dades sensibles**.

Per tant, el consentiment ha de ser **verificable** i qui recopili dades personals hauran de poder provar que el afectat els hi va concedir el seu consentiment.

Avaluacions d'Impacte en la Protecció de Dades

Què és una Avaluació d'Impacte en la Protecció de Dades?

És principalment, **un exercici d'anàlisis dels riscs** que un determinat sistema d'informació, producte o servei pot suposar per el dret a la protecció de dades dels afectats dels que es tracten les seves dades, i com resultat d'aquest anàlisis, la gestió dels mencionats riscs mitjançant l'adopció de les mesures encasaries per eliminar o atenuar en lo possible aquells que se hagin identificat.

Les seves sigles en anglès son PIA, que corresponen a "*Privacy Impact Assessment*".

RGPD

Una de les principals novetats que incorpora el nou Reglament General de Protecció de Dades, concretament en el article 35, es la obligació de realitzar una EIPD d'aquells tractaments que puguin comportar un risc significatiu (alt) per els drets i les llibertats de les persones físiques.

L'article mencionat utilitza la expressió "en particular", amb el que es dedueix que no estem davant una llista exhaustiva; per tant, hi ha altres tipus de tractaments que no encaixen en aquests supòsits i que també poden presentar riscos igualment elevats i, en conseqüència, s'haurà de fer la EIPD.

Anàlisis de riscos de protecció de dades

L'objectiu del anàlisis de riscos és **determinar la probabilitat de que se produeixin situacions no desitjades i la seva gravetat**. Per tant, concretarem i descriurem quines mesures s'han previst per els processos clau del tractament que estem avaluant.

S'haurà d'**analitzar** també les diferents mesures que se han previst inicialment per reduir els riscos del tractament (en les seves dues dimensiones: probabilitat i gravetat). D'aquesta forma, podrem valorar el nivell de risc inicial de las operacions de tractament que s'han dissenyat.

Si no es pren cap tipus de mesura per mitigar la probabilitat i la gravetat d'un potencial escenari de risc, es altament probable que es produeixi i, a priori, pot tenir unes conseqüències molt greus (el nivell de risc es valora en la següent etapa de avaluació dels riscs).

Finalitat de una EIPD

L'objectiu d'una EIPD és **permetre als responsables del tractament prendre mesures adequades** per reduir el risc (minimitzar la probabilitat de la seva materialització i les conseqüències negatives per els interessats).

Destacar, en aquest sentit, que las EIPD han de fer-se abans d'iniciar les operacions del tractament; essent el primer pas la determinació de la necessitat (o no) del anàlisis de la avaluació d'impacte.

Quan s'ha de realitzar la Avaluació d'Impacte de Protecció de Dades?

No sempre es necessària la redacció d'una Avaluació d'Impacte, encara que és recomanable que a l'hora de realitzar un nou tractament sempre s'analitzin els possibles riscos que pot suposar.

No obstant, la nova regulació europea diu **que es obligatòria** quan es doni:

- Risc elevat
- Avaluació sistemàtica
- Tractament a gran escala de dades especialment protegides
- Ús de tecnologies invasives

Risc Elevat

Quan el tractament pugui tenir un alt risc per els drets i llibertats de las persones físiques.

Per exemple en la utilització de noves tecnologies, o si ens atenem a la seva naturalesa, context i dimensió.

Avaluació sistemàtica

En el moment que, sistemàticament, s'avaluïn aspectes personals de persones físiques basat en un tractament automatitzat

És el cas de la elaboració de perfils.

Tractament a gran escala de dades especialment protegides

Si es realitza un tractament a gran escala de las categories especials de dades del article 9, apartat 1 del RGPD, o de los dades personals relatives a condemnes i infraccions penals a les que es refereix l'article 10 del RGPD. Inclourem en aquest apartat també les dades personals relatives a menors.

Ús de tecnologies invasives

Si s'utilitzen tecnologies que es consideren especialment invasives amb la privacitat com:

- Vídeo vigilància a gran escala
- Aeronaus no tripulades (Drons)
- Vigilància Electrónica
- Mineria de dades
- Biometria
- Tècniques genètiques
- Geolocalització

Empreses obligades a realitzar una Avaluació d'Impacte:

- Farmacèutiques
- Hospitals y clíniques
- Seguretat privada, vigilància y control
- Comercialitzadores d'energia
- Empreses que realitzen comerç electrònic
- Col·legis

Contingut

El resultat final de una avaluació d'impacte no deixa de ser un informe, o un conjunt de documentació, que recull les característiques del tractament avaluat i les decisions adoptades per mitigar els seus riscos, d'acord amb la seva identificació, anàlisis, valoració i tractament (gestió de riscos), y una vegada analitzades també les qüestions com el interès legítim (si s'escau) o la necessitat i la proporcionalitat de les operacions del tractament.

L'article 35.7 del RGPD concreta quin ha de ser el contingut mínim de la avaluació o, si es prefereix, determina quines qüestions es tenen d'analitzar, como mínim, per considerar que s'ha fet la avaluació de manera adequada.

Questions que obligatòriament es tenen d'analitzar:

Descripció del tractament i finalitats

S'haurà de portar a terme un anàlisis en profunditat del projecte, obtenint el detall de las categories de les dades que es tracten, els usuaris que les tracten, els fluxos d'informació i les tecnologies utilitzades.

Avaluació de la proporcionalitat i necessitat del tractament

Les autoritats de protecció de dades habitualment assenyalen que per comprovar si una operació de tractament suposa una mesura restrictiva d'un dret fonamental, aquesta operació té de superar els tres punts del anomenat judici de proporcionalitat:

Judici d' idoneïtat

Que la mesura pugui aconseguir l'objectiu proposat.

Judici de necessitat

Si, a més, és necessària, en el sentit de que no existeix cap altra manera més moderada per aconseguir aquest propòsit amb la mateixa eficàcia.

Judici de proporcionalitat en sentit estricte

Si la mesura es ponderada o equilibrada, per que se'n deriven més beneficis o avantatges per el interès general que no perjudicis sobre altres bens o valors en conflicte.

Per tant, la proporcionalitat té a veure amb avaluar si la finalitat que se persegueix es pot aconseguir per altres mitjans, per exemple: utilitzant altres dades (o menys dades), reduint el col·lectiu de persones afectades (quantitativament o qualitativament parlant), utilitzant altres tecnologies menys invasives o aplicant altres procediments o mitjans de tractament modificant els inicialment previstos, etc.

Avaluació dels riscos

S'ha de portar a terme un anàlisis dels possibles riscos per la protecció de dades dels afectats i valoració de la probabilitat i el impacte de la seva materialització.

Mesures previstes

Un cop analitzats els riscos s'han d'establir **mesures per afrontar-los.**

Es a dir, s'han d'establir garanties en funció dels mateixos mitjançant amb les que es garanteixi la protecció de los dades personals, així com també que tots els procediment compleixen escrupolosament amb la normativa (RGPD), sempre sense perdre de vista els drets i interessos legítims de los interessats y de altres persones afectades.

Quin és el paper del Delegat de Protecció de Dades respecte a las EIPD?

En primer lloc, dir que el RGPD determina que quan el responsable del tractament ha de portar a terme una EIPD ha de buscar el assessorament del DPO.

Aquest recolzament el podem entendre tant com una intervenció activa en el disseny i execució de la avaluació, amb funcions de coordinació o de interlocució principal amb els avaluadors, o bé de col·laboració amb el avaluador, si resulta que no ha d'assumir un paper principal en la EIPD.

En aquest últim cas queda com persona de contacto rellevant dins de la organització i ha d'atendre les consultes i donar el recolzament que el responsable del tractament determini en cada cas.

Anàlisis de riscos en la Protecció de Dades

Què es un risc?

Es pot definir como l**a combinació de la possibilitat** de que se materialitzi una amenaça i **les seves conseqüències negatives**.

Per tant el **nivell del risc** es determina segons la seva probabilitat de materialitzar-se i el impacte que té en el cas de fer-ho.

Què és un anàlisis de riscos?

Degut a la constant evolució tecnològica i, per tant, la transformació digital que sofreixen els tractaments de dades personals es fa necessari que s'adopti una actitud dinàmica, enfocada a la gestió de los riscos potencials associats.

Per tant, el ***anàlisis de riscos*****,** és el **anàlisis previ que s'ha de fer a tot nou tractament de dades personals amb la principal finalitat d'establir els controls i mesures de seguretat adequades que garanteixin les llibertats i els drets de les persones afectades.**

Cal destacar que per avaluar un risc es necessari considerar tots els possibles escenaris amb els que el risc es faria efectiu, inclosos aquells que impliquen un mal ús o abús de les dades i les alteracions tècniques o del entorn.

Qui ha de realitzar el anàlisis de riscos?

Un dels principals punts a tenir en compte es **qui**, dins de l'entitat, s'**encarregarà de realitzar el anàlisis dels riscos.**

En aquelles empreses que contin amb la figura del **Delegat de Protecció de Dades,** serà aquet el encarregat de portar-lo a terme.

Sí la empresa no disposa d'aquesta figura, s'haurà de designar a un encarregat per tal de realitzar aquesta tasca en funció dels seus coneixements en la matèria.

No obstant s'ha de destacar que no solsament se encarregarà una persona de portar-lo a terme, sinó que la persona designada s'haurà de coordinar amb tot el personal de l'entitat que pugui estar involucrat en els tractaments i serveis.

On es troba regulat?

Ni en el RGPD ni en la nova *Ley Orgánica de Protección de Datos* conté un article expressament denominat anàlisis de riscos.

No obstant, la necessitat de la realització d'aquest anàlisis el podem deduir dels següents articles:

Apartat 1 del **article 25 del RGPD**:

"*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 pseudonimización, 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*".

Apartat 2 del **article 25 del 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".*

Apartat 2 del **article 32 del RGPD**:

"Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento 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 autorizados a dichos datos."

És el mateix un anàlisis de riscos que una Avaluació de Impacte?

No, són dos procediments diferents encara que complementaris.

El **anàlisis de riscos** té a veure amb la determinació de la pèrdua potencial per causa d'una amenaça i el cost de la mesura de protecció envers a les dades personals emprades en l'organització.

Es a dir, quant gastar en prevenció y protecció. Per això, es necessita saber primer quins són aquests processos i recursos crítics.

Per comptes, en la **Avaluació d' Impacte** es busca principalment:

- Determinar el impacte que tindria un esdeveniment disruptiu en les dades personals de la organització.
- Identificar los recursos, persones, infraestructura física, tecnològica, informació i tercers dels que depenen.

Per altra part, en el **anàlisis de riscos**, s'identifiquen les amenaces de interrupció més probables i s'analitzen les vulnerabilitats relacionades amb les amenaces avaluant els controls de seguretat física, lògica i ambiental, revisant la seva efectivitat per contenir les amenaces identificades, mentre que en la **Avaluació d'Impacte** s'analitzen els riscos que un sistema, producte o servei poden suposar per els drets i llibertats de les persones i, després d'haver realitzat aquest anàlisis, es gestionen els perills abans de que se materialitzin.

Com realitzar un anàlisis de riscos

Quan anem a realitzar un anàlisis de riscos haurem de partir de set fases clares per poder fer-la amb garanties.

No obstant s'ha de tenir en compte que s'haurà de tractar sempre un **model flexible**, es a dir, que es pugui adequar a les diferents estructures de les organitzacions.

Aquestes **set fases** son las següents:

1. Necessitat del anàlisis

Es primordial conèixer les **raons** por las que hem d'executar un Anàlisis dels riscos d'un tractament de dades personals.

De buscar aquestes raons se'n encarregarà el DPO, no obstant en el cas de que en l'entitat no tingui aquesta figura, es tan fàcil como **contestar a las següents preguntes:**

- ¿Es recapten dades de caràcter personal?
- ¿Aquestes dades es comuniquen a tercers?
- ¿Es fa servir tecnologia invasiva per la privacitat en el tractament?
- ¿Es tracten dades considerades especialment protegides?
- ¿Les dades que han sigut recaptades s'utilitzaran de forma massiva per accions de *marketing*?

En el cas de que **la resposta sigui afirmativa** en tots els cassos haurem de realitzar un anàlisis dels riscos en el tractament de dades personals.

2. Descripció dels fluxos d'informació

El segon pas es conèixer tots allò relacionat amb el tractament de les dades personals, es a dir:

- com es recapten les dades
- per a que es volen utilitzar
- amb quina finalitat
- persones amb accés a la informació.

3. Identificació dels riscos que afecten a la privacitat

En el tercer pas ja s'han d'identificar els riscos que puguin donar-se al tractar les dades personals.

Poden ser de tres **tipus**:

- **sobre els afectats** (com la invasió en la seva vida privada, comunicar dades a tercers quan no sigui necessari, no haver realitzat un procediment adequat de anonimització, mantindre les dades més temps del estrictament necessari per a la finalitat per la que es varen recollir).
- **riscos corporatius** (com pèrdua de reputació o una multa por esquerdes de seguretat).
- **legals** (com no complir amb la legislació de protecció de dades, o serveis de la societat de la informació).

4. Establiment de solucions que garanteixin la privacitat

Identificats cada un dels riscos, a continuació s'hauran de **desenvolupar les solucions** o mesures corresponents para **mitigar i/o eliminar** els riscos detectats.

Cal destacar que si lo idoni és la eliminació dels riscos, en certs casos no serà necessari, permetent la normativa reduir-los a un nivell acceptable que permeti a la empresa tractar amb seguretat les dades personals.

La realització d'un Anàlisis de riscos no té per què eliminar completament els riscos sobre la privacitat dels afectats, sinó reduir-los a un nivell acceptable que permeti a la organització la implementació del producte, servei o tractament de dades personals.

Al mateix temps, s'ha de **valorar el cost i benefici** d'implementar aquestes solucions, tenint en compte que en alguns casos, existirà un cost econòmic, pel que s'haurà de realitzar una comparativa entre costos i beneficis (*per exemple, sobre las mesures de seguretat que puguin evitar una fuga de dades personals i conseqüentment, una pèrdua de reputació per la empresa).*

5. Implementació de solucions prèviament establertes

Un cop que **ja s'han establert les solucions** que es puguin adoptar per reduir o eliminar el risc detectat, s'ha de **decidir quines s'implementaran.**

Com ja s'ha comentat, no es necessari que se apliquen totes las solucions, sinó que **s'apliquin les mesures per els riscos que siguin inacceptables per la entitat.**

A més d'implementar les solucions, es important **registrar cada un dels riscos i les solucions** adoptades, així com qui és el responsable de posar-les en funcionament.

Tot això s'haurà d'incloure en un **informe final** del anàlisis, el qual, com bona pràctica es recomanable que sigui publicat a fi de donar una major transparència i que els afectats sàpiguen com afecta el producte, servei o tractament, a la seva privacitat.

6. Participació de les parts implicades

És necessària que en totes las fases anteriorment descrites la informació entre els diferents departaments i agents implicats sigui fluida per aconseguir plenament el objectiu del anàlisis de riscos que és prevenir els potencials riscos detectats per tal de garantir la màxima cura en el tractament de les dades personals que custodia l'entitat i/o empresa.

7. Integració del anàlisis de riscos en la gestió

Intentar, en la mesura del possible, que el Anàlisis de riscos formi part de la pròpia gestió de l'empresa / organització, ja que es la forma més segura de **garantir la privacitat** de productes y serveis.

DIFERENCIES ENTRE:

LA LOPD (1999 – 2018)	RGPD (2018)
Registre dels fitxers en AEPD	Registre de les activitats del tractament
Registre d'incidències	Comunicació en 72H de les incidències
Comunicació drets ARCO	Ampliació drets al oblit i a la portabilitat
Responsable de Seguretat	Delegat de protecció de dades
Informe d'auditoria	Avaluació d'impacte
Sancions de 900€ a 600000€	Del 2% al 4% de Factur. Fins a20 Milions €
Consentiment tàcit	Consentiment inequívoc
Signatura contracte amb encarregat	Certificat conforme compleix a normativa

Complir amb el RGPD de Protecció de Dades Personals

Per tal de gestionar i obtenir un document de seguretat bàsic la AEPD ofereix un servei WEB on al complimentar les dades que es demanen, es genera automàticament un document editable (tipus WORD) per tal de complir amb els requeriments mínims indispensables del RGPD.

http://www.servicios.agpd.es/Facilita

Accions a fer necessàries i recomanables:

a) Comunicar a clients, proveïdors, treballadors els seus drets en protecció de dades.
b) Actualitzar o fer nous contractes d'encàrrec de tractament de dades i signar-los.
c) Realitzar un **Registre d'activitats del tractament** (abans Document de Seguretat) i si és necessària una avaluació de impacte, actualment no obligatòria en entitats on no es tracten dades especialment protegides, per tal de tenir una visió global del sistema informàtic de l'empresa i de qui té accés a les dades personals que aquesta emmagatzema així com dels possibles riscos.
Per qualsevol consulta o assessorament podeu enviar un correu electrònic a :
gbinfor@gbinfor.com