

DIPUTACIÓ DE
VALÈNCIA



Protecció de Dades i Seguretat de la Informació



Butlletí protecció de dades

Butlletí del Departament de protecció de dades i Seguretat
de la Informació de la Diputació Provincial de València

Butlletí N.º 17 | Novembre 2021

**PRINCIPIS BÀSICS EN EL TRACTAMENT DE DADES
DE CARÀCTER PERSONAL**



Í N D E X



PRINCIPIS BÀSICS EN EL TRACTAMENT DE DADES DE CARÀCTER PERSONAL

	Pág.
Introducció.....	3
• Principis relatius al tractament	4
• Responsabilitat Proactiva	5
• Mesures a tindre en compte	7
Material complementari	8
Notícies d'actualitat	8



Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interès per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades i
Seguretat de la Informació

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONS

Si desitges subscriure's al nostre
Butlletí informatiu accedeix al
següent [enllaç](#)



INTRODUCCIÓ

Existeixen determinats principis que han de tindre presents totes les organitzacions a l'hora de tractar **les nostres dades de caràcter personal**. Aquests principis es troben regulats en l'article 5 del Reglament (UE) 2016/679 General de Protecció de Dades (d'ara en avant, RGPD) i, de manera connexa, en determinats preceptes de la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (d'ara en avant , LOPDGDD).

Els **principis protecció de dades** són: (i) Licitud, lleialtat i transparència, (ii) Limitació de la finalitat, (iii) Minimització de les dades, (iv) Exactitud, (v) Limitació del termini de conservació, (vaig veure) Integritat i confidencialitat i (vii) responsabilitat Proactiva.

En aquest butlletí analitzarem un a un els principis protecció de dades i com han de ser interpretats.

Cal destacar, que el RGPD introdueix un canvi dràstic en matèria de responsabilitat que es projecta sobre totes les obligacions a les quals està sotmeses el Responsables del Tractament, es tracta del principi de Responsabilitat Proactiva o accountability.

El RGPD descriu aquest principi com la necessitat que els responsables del tractament apliquen mesures tècniques i organitzatives apropiades, no sols per a garantir el compliment de la normativa, sinó també per a demostrar davant els interessats i autoritats de supervisió, aquest compliment.

La qual cosa es tradueix en l'exigència d'una major implicació per part dels responsables i els encarregats amb una actitud proactiva i conscient.





PRINCIPIS RELATIUS AL TRACTAMENT

Quan parlem de Principis, entenem com a tals el que disposa el art.5 del RGPD;

“Article 5: Principis relatius al tractament

1. *Les dades personals seran:*

- a. *tractats de manera lícita, lleial i transparent en relació amb l'interessat («licitud, lleialtat i transparència»);*
- b. *recollits amb fins determinats, explícits i legítims, i no seran tractats ulteriorment de manera incompatible amb aquests fins; d'acord amb l'article 89, apartat 1 (Investigació Científica, estadística), el tractament ulterior de les dades personals amb finalitats d'arxiu en interès públic, fins d'investigació científica i històrica o fins estadístics no es considerarà incompatible amb els fins inicials («limitació de la finalitat»);*
- c. *adequats, pertinents i limitats al necessari en relació amb els fins per als quals són tractats («minimització de dades»);*
- d. *exactes i, si fora necessari, actualitzats; s'adoptaran totes les mesures raonables perquè se suprimisquen o rectifiquen sense dilació les dades personals que siguin inexactes respecte als fins per als quals es tracten («exactitud»);*
- e. *mantinguts de manera que es permeta la identificació dels interessats durant no més temps del necessari per als fins del tractament de les dades personals; les dades personals podran conservar-se durant períodes més llargs sempre que es tracten exclusivament amb finalitats d'arxiu en interès públic, fins d'investigació científica o històrica o fins estadístics, de conformitat amb l'article 89 (Investigació Científica, estadística), apartat 1, sense perjudici de l'aplicació de les mesures tècniques i organitzatives apropiades que imposa el present Reglament a fi de protegir els drets i llibertats de l'interessat («limitació del termini de conservació»);*
- f. *tractats de tal manera que es garantisca una seguretat adequada de les dades personals, inclosa la protecció contra el tractament no autoritzat o il·lícit i contra la seua pèrdua, destrucció o mal accidental, mitjançant l'aplicació de mesures tècniques o organitzatives apropiades («integritat i confidencialitat»).*

2. *El responsable del tractament serà responsable del compliment del que es disposa en l'apartat 1 i capaç de demostrar-lo («responsabilitat proactiva»).*”

Considerant 39; “Tot tractament de dades personals ha de ser lícit i lleial. Per a les persones físiques ha de quedar totalment clar que s'estan recollint, utilitzant, consultant o tractant d'una altra manera dades personals que els concerneixen, així com la mesura en què aquestes dades són o seran tractats. El principi de transparència exigeix que tota informació i comunicació relativa al tractament d'aquestes dades siga fàcilment accessible i fàcil d'entendre, i que s'utilitze un llenguatge senzill i clar. Aquest principi es refereix en particular a la informació dels interessats sobre la identitat del responsable del tractament i els fins del mateix i a la informació afegida per a garantir un tractament lleial i transparent respecte a les persones físiques afectades i al seu dret a obtindre confirmació i comunicació de les dades personals que els concernisquen que siguin objecte de tractament. [...]”



Els principis generals de la protecció de dades de caràcter personal, no sols són mers fonaments pels quals s'ha de regir l'elaboració, interpretació i aplicació de la normativa sobre protecció de dades, sinó que es tracta d'un conjunt de regles que determinen com recollir, tractar i cedir les dades.

En cas de trobar-nos amb llacunes o buits legals, ens hem d'inspirar en aquests, perquè el tractament de les dades siga conforme a la normativa.

En definitiva, són deures i obligacions als quals estan subjectes els tractaments de dades de caràcter personal.

Els principis recollits en el RGPD [semblants als disposats en la predecessora legislació, europea i espanyola] són com abans hem ja avançat, els següents:

“Considerant 40: Perquè el tractament siga lícit, les dades personals han de ser tractats amb el consentiment de l'interessat o sobre alguna altra base legítima establida conforme a Dret, ja siga en el present Reglament o en virtut de 4.5.2016 ÉS Diari Oficial de la Unió Europea L 119/7 un altre Dret de la Unió o dels Estats membres a què es referisca el present Reglament, inclosa la necessitat de complir l'obligació legal aplicable al responsable del tractament o la necessitat d'executar un contracte en el qual siga part l'interessat o a fi de prendre mesures a instàncies de l'interessat amb anterioritat a la conclusió d'un contracte.”

- **Lleialtat** – No poden recaptar-se dades personals per mitjans fraudulents (això és, no podran utilitzar mitjans o mètodes enganyosos) deslleials (que donen lloc a una discriminació injusta o arbitrària contra els titulars) i il·lícits (és a dir, que siguen il·legals, estiguen fora o al marge de la Llei).
- **Transparència** – Exigeix que tota informació i comunicació relativa al tractament de dades personals siga fàcilment accessible i fàcil d'entendre, i que s'utilitze un llenguatge senzill i clar
- **Licitud o legitimació del tractament.**- Perquè el tractament siga lícit, les dades personals han de ser tractats amb el consentiment explícit de l'interessat o sobre una altra base o fonament jurídic (article 6 RGPD).
- **Limitació de la finalitat.**- Les dades personals han de ser recollits amb finalitats determinats, explícits i legítims, i no seran tractats, posteriorment, de manera incompatible o diferent amb aquests fins.
- **Minimització.**- Han de ser adequats, pertinents i limitats o no excessius, en relació amb els fins que legitimen el tractament.
- **Exactitud.**- Les dades han de ser exactes i, si fora necessari, actualitzats. Han d'adoptar-se totes les mesures raonables per a corregir errors, modificar les dades que resulten ser inexactes o incomplets i garantir la certesa de la informació objecte de tractament.
- **Limitació del termini de conservació.**- No podran conservar-se o mantindre's les dades durant més temps del necessari per als fins del tractament. Han d'establir-se terminis per a la supressió o revisió periòdica.
- **Integritat i confidencialitat.**- Ha de garantir-se una seguretat adequada per a preservar la integritat de les dades i impedir l'accés o ús no autoritzat. Totes les persones que intervinguen en qualsevol fase del tractament estan subjectes a guardar secret o confidencialitat amb caràcter indefinit

RESPONSABILITAT PROACTIVA

Com avançàvem en la introducció, el RGPD ens introdueix el principi denominat “responsabilitat proactiva”, expressió que pretén traduir el terme anglés “accountability”, segons el qual els responsables aplicaran les mesures tècniques i organitzatives apropiades per a garantir i estar en condicions de demostrar que el tractament de dades personals es duu a terme de conformitat amb el Reglament.



Abans d'entrar a veure el principi de responsabilitat proactiva en el (RGPD), cal indicar que el Grup de Treball de l'Article 29 (GT29), que va ser substituït després de la plena aplicació del RGPD (el 25 de maig) pel Comitè Europeu de Protecció de Dades (CEPD), va publicar en 2010 el Dictamen 3/2010 sobre el principi de responsabilitat, WP173, en el qual explicava el seu significat i abast.

El GT29 assenyalava que «prové del món anglosaxó on és d'ús general i on es dona una comprensió àmpliament compartida del seu significat, encara que la definició exacta de «responsabilitat» resulta complexa en la pràctica.» I també que «el terme apunta sobretot a la manera en què s'exerceixen les competències i a la manera en què això pot comprovar-se.»

Com assenyalava l'AEPD (Principi Responsabilitat Proactiva) el RGPD, en el seu article 24, descriu aquest principi com la necessitat que el responsable del tractament aplique mesures tècniques i organitzatives apropiades a fi de garantir i poder demostrar que el tractament és conforme amb el Reglament.

Per a això les organitzacions han d'analitzar quines dades tracten, amb quines finalitats ho fan i quin tipus d'operacions de tractament duen a terme, per a passar a realitzar l'Anàlisi de Riscos.

Així doncs en parlar de Responsabilitat proactiva o accountability ens centrats en dos elements:

1. La necessitat que el responsable del tractament adopte mesures adequades i eficaces per a aplicar els principis de protecció de dades.

Mesures tècniques i organitzatives que seran revisades i actualitzades, és a dir, el responsable del tractament haurà d'avaluar o analitzar en tot moment el risc, atenent també qualsevol canvi en el mateix ja siga, per exemple, per nous tractaments de dades personals

2. La necessitat de demostrar, si així es requereix, que s'han adoptat mesures adequades i eficaces. En aquest cas s'aconsegueix recaptant evidències, documentant actuacions que podran ser de prova davant incidents

Finalment assenyalava que la responsabilitat proactiva s'exigeix al responsable del tractament amb independència de què tracte les dades personals per si mateix o a través d'un encarregat del tractament o subencarregats de tractament.

MESURES A TINDRE EN COMPTE

El principi de responsabilitat proactiva o accountability posa en relleu la necessitat de donar visibilitat a les bones pràctiques en la protecció de dades, la qual cosa es manifesta en el article 42 del Reglament, però **Quines mesures trobem en el RGPD l'aplicació del qual suposa que les organitzacions estan sent proactives en l'adopció de mesures de seguretat?**



Els Estats membres, les autoritats de control, el Comitè i la Comissió promouran la creació de mecanismes de certificació en matèria de protecció de dades i de segells i marques de protecció de dades a fi de demostrar el compliment del que es disposa en el Reglament en les operacions de tractament dels responsables i els encarregats.



L'establiment de mecanismes de certificació i segells de qualitat, permet avaluar ràpidament el nivell de protecció d'una empresa.

El RGPD també posa l'accent en la rendició de comptes eficaç en parlar de les següents mesures, entre altres:

- Registre d'activitats: nova obligació de documentació del tractament per als responsables o els encarregats que han de dur a terme un registre de totes les activitats de tractament que realitzen.
- Protecció de dades des del disseny: el responsable aplicarà, tant en el moment de determinar els mitjans de tractament com en el tractament mateix, les mesures tècniques i organitzatives adequades per a oferir les garanties necessàries i complir els requeriments del Reglament.
- Protecció de dades per defecte: el responsable aplicarà les mesures tècniques i organitzatives adequades per a garantir que, per defecte, només es tracten les dades personals necessàries per a cada finalitat específica del tractament.
- Mesures de seguretat: el RGPD no estipula un llistat de les mesures de seguretat a aplicar, sinó que estableix que el responsable siga qui decidisca quines mesures tècniques i organitzatives són les adequades segons el risc que comporta el tractament.
- Avaluacions d'Impacte: quan siga probable que un tractament, especialment si s'utilitzen les noves tecnologies, per la seua naturalesa, abast, context o finalitats, supose un alt risc per als drets i llibertats de les persones físiques, el responsable ha de realitzar una avaluació de l'impacte.
- Autorització prèvia o consultes prèvies: si després de l'avaluació d'impacte s'observa que el tractament previst podria infringir el RGPD, el responsable ha de fer una consulta a l'autoritat de control per a conèixer la manera correcta de conducta.
- DPD: és l'encarregat d'informar i assessorar el responsable o a l'encarregat i als treballadors sobre les obligacions que imposa la normativa, supervisar el seu compliment, assessorar sobre l'avaluació d'impacte i cooperar amb l'autoritat de control, entre altres tasques.
- Notificació de violació de seguretat: si es produeix una violació de la seguretat, el responsable ha de notificar-lo a l'autoritat de control en un termini màxim de 72 hores, i de ser el cas als afectats



MATERIAL COMPLEMENTARI

- Guia de l'AEPD "Guia de Privacitat des del Disseny". Consulta la guia en [aquest enllaç](#).
- Guia de Protecció de Dades per Defecte (AEPD). Consulta la guia en [aquest enllaç](#).
- Gestió del risc i avaluació d'impacte en tractaments de dades personals (AEPD). Consulta la guia en [aquest enllaç](#).
- Guia per a la gestió i notificació de bretxes de Seguretat (AEPD). Consulta la guia en [aquest enllaç](#).
- Guia del Reglament General de Protecció de Dades per a Responsables de Tractament (AEPD). Consulta la guia en [aquest enllaç](#).
- GRUP DE TREBALL SOBRE PROTECCIÓ DE DADES DE L'ARTICLE 29 va publicar en 2010 el Dictamen 3/2010 sobre el principi de responsabilitat, WP173, en el qual explicava el seu significat i abast. Consulta el dictamen en [aquest enllaç](#).

NOTÍCIES

- **Les empreses informatives i les agències de notícies podran negociar de manera independent amb les grans tecnològiques com Google i Facebook una remuneració per la difusió dels seus continguts en línia** sempre que aquestes obtinguen una autorització prèvia i l'acord entre les dues parts es faça amb "bona fe contractual, diligència deguda, transparència i respecte a les regles de la lliure competència, excloent l'abús de posició de domini en la negociació". Consulta l'article en [aquest enllaç](#).
- **L'AEPD adverteix que els registres de dades biomètriques de les jornades laborals són invasius:** Els registres de jornada de caràcter biomètrics són molt invasius i manegen massa dades personals, segons l'AEPD que en una recent resolució, finalitzada per pagament voluntari, sanciona a Serveis Logístics Martorell Segle XXI amb 20.000 euros per la implantació d'aquest registre al seu client automobilístic SEAT. Consulta l'article en [aquest enllaç](#).
- **L'AEPD aborda en el seu blog Anonimització i seudonimització (II): la privacitat diferencial.** En la cerca d'un equilibri entre l'explotació legítima de la informació i el respecte als drets individuals han sorgit estratègies encaminades a preservar la utilitat de les dades al mateix temps que es respecta la privacitat de les persones. Una d'elles és la privacitat diferencial, que tracta d'establir garanties de protecció de dades des del disseny mitjançant la implementació pràctica d'estratègies d'abstracció de la informació, així és com ho aborda l'Agència en aquest blog. Consulta el blog en [aquest enllaç](#).