Diputació de València | Protecció de Dades i Seguretat de la Informació

Quaderns DivalData

Quaderns dirigits a delegats,
responsables i especialistes en protecció
de dades personals

Quadern N.º 41 | Novembre 2023

LA PRIVACITAT PER DISSENY I PER DEFECTE

ÍNDEX

LA PRIVACITAT PER DISSENY I PER DEFECTE

INTRODUCCIÓ.....2

1. NATURALESA I CONSIDERACIÓ DEL TRACTAMENT 3

2. PRINCIPIS FUNDACIONALS DE LA PRIVACITAT DES DEL DISSENY 6

3. OBJECTIUS DE SEGURETAT DE LA PRIVACITAT DES DEL DISSENY.....7

4. CICLE DE VIDA DE LA PRIVACITAT DES DEL DISSENY.....8

5. ESTRATÈGIES, PATRONS I TÈCNIQUES DE LA PRIVACITAT 9

6. PRIVACITAT PER DEFECTE 12

7. CONCLUSIONS.....13

NOTÍCIES.....15

Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interés per als pròxims quaderns. Estes peticions hauran de dirigir-se a:

Diputació de València

Departament de Protecció de Dades i Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUBSCRIPCIONS

Si desitges subscriure's al nostre Quadern accedeix al següent enllaç.

"La privacitat per disseny i per defecte es troba regulada en el considerant 78 i article 25 del RGPD, així com en l'article 28 de la LOPDGDD".

INTRODUCCIÓ

La normativa en protecció de dades, en particular, el Reglament Europeu de Protecció de Dades (RGPD) i la Llei orgànica 3/2018 de Protecció de dades i Garantia de drets digitals (LOPDGDD) obliga als responsables del tractament una configuració per disseny i per defecte dels tractaments que siga respectuosa amb els principis de protecció de dades.

La privacitat per disseny i per defecte es troba regulada en el considerant 78 i article 25 del RGPD, així com en l'article 28 de la LOPDGDD.

A continuació, es desenvolupa la privacitat per disseny de forma més exhaustiva, incloent-hi els principis fundacionals de la privacitat, els nous objectius de protecció específics de la privacitat, el cicle de vida de la privacitat per disseny, així com las diferents estratègies, patrons i tècnicas per a garantir la privacitat de les nostres dades.

Finalment, es detalla la definició de la protecció de dades per defecte (d'ara en avant, PDpD) i les implicacions que comporten en una auditoria. Així mateix, desenvolupem el concepte de patrons foscos i expliquem on pot trobar-se una llista orientativa de mesures per defecte per a aplicar a la nostra entitat i complir amb els principis en matèria de protecció de dades.

Nota.- Una part del contingut mostrat, a continuació, és extracte de publicacions fetes de les autoritats de control en protecció de dades. Es tracta d'una síntesi feta per a saber i entendre què signifiquen estos principis en l'àmbit de la protecció de dades de caràcter personal.

"Els principis de la protecció de dades des del disseny i per defecte també han de tindre's en compte en el context dels contractes públics".

1. NATURALESA I CONSIDERACIÓ DEL TRACTAMENT

El Considerant 78 del Reglament (UE) 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'estes dades (RGPD) ja anticipa el concepte de privacitat per disseny i per defecte i estableix que:

"La protecció dels drets i llibertats de les persones físiques respecte al tractament de dades personals exigeix l'adopció de mesures tècniques i organitzatives apropiades amb la finalitat de garantir el compliment dels requisits del present Reglament. A fi de poder demostrar la conformitat amb el present Reglament, el responsable del tractament ha d'adoptar polítiques internes i aplicar mesures que complisquen en particular els principis de protecció de dades des del disseny i per defecte. Aquestes mesures podrien consistir, entre altres, a reduir al màxim el tractament de dades personals, seudonimizar al més prompte possible les dades personals, donar transparència a les funcions i el tractament de dades personals, permetent als interessats supervisar el tractament de dades i al responsable del tractament crear i millorar elements de seguretat. En desenvolupar, dissenyar, seleccionar i usar aplicacions, serveis i productes que estan basats en el tractament de dades personals o que tracten dades personals per a complir la seua funció, ha d'encoratjar-se als productors dels productes, serveis i aplicacions al fet que tinguen en compte el dret a la protecció de dades quan desenvolupen i dissenyen estos productes, serveis i aplicacions, i que s'asseguren, amb la deguda atenció a l'estat de la tècnica, que els responsables i els encarregats del tractament estan en condicions de complir les seues obligacions en matèria de protecció de dades. Els principis de la protecció de dades des del disseny i per defecte també han de tindre's en compte en el context dels contractes públics".

"El responsable del tractament aplicarà, abans i durant el tractament, mesures tècniques i organitzatives apropiades per al compliment dels principis i requisits del Reglament Europeu de Protecció de dades".

Així mateix, el article 25 del Reglament (UE) 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'estes dades (RGPD), sota la rúbrica "*Protecció de dades des del disseny i per defecte*", disposa en el primer apartat que:

> *"Tenint en compte l'estat de la tècnica, el cost de l'aplicació i la naturalesa, àmbit, context i fins del tractament, així com els riscos de diversa probabilitat i gravetat que comporta el tractament per als drets i llibertats de les persones físiques, el responsable del tractament aplicarà, tant en el moment de determinar els mitjans de tractament com en el moment del propi tractament, mesures tècniques i organitzatives apropiades, com la seudonimización, concebudes per a aplicar de manera efectiva els principis de protecció de dades, com la minimització de dades, i integrar les garanties necessàries en el tractament, a fi de complir els requisits del present Reglament i protegir els drets dels interessats".*

D´esta definició de privacitat per disseny (d'ara en avant, PbD; per les sigles de l'anglés *Privacy by Design*) es poden extraur cinc característiques principals:

a) La privacitat per disseny està orientada **a la gestió del risc** amb un plantejament dinàmic i de millora contínua per a determinar les mesures tècniques i organitzatives a implantar en l'entitat.

b) La privacitat per disseny està orientada **a la responsabilitat proactiva** del responsable del tractament que realitza una anàlisi crítica, continu i traçable en el compliment de les obligacions en matèria de protecció de dades.

c) La privacitat per disseny està relacionada amb els principis de protecció de dades, i especialment , al princip**i de minimització de dades**.

"El responsable del tractament aplicarà mesures tècniques i organitzatives apropiades que per defecte siguen objecte del tractament de dades personals i per als fins específics".

d) Les mesures apropiades a aplicar per a complir la privacitat per disseny han de tindre caràcter **tècnic, però també organitzatiu**.

e) Les mesures tecniques i organitzatives han d'adoptar-se **abans** d'iniciar el tractament i, també, **durant** del tractament.

Il·lustració 1. - Privacitat des del disseny

A continuació, en el segon apartat de l'article 25 es defineix la privacitat per defecte i indica que: *"El responsable del tractament aplicarà les mesures tècniques i organitzatives apropiades amb la intenció de garantir que, per defecte, només siguen objecte de tractament les dades personals que siguen necessaris per a cadascun dels fins específics del tractament. Esta obligació s'aplicarà a la quantitat de dades personals recollits, a l'extensió del seu tractament, al seu termini de conservació i a la seua accessibilitat. Tals mesures garantiran en particular que, per defecte, les dades personals no siguen accessibles, sense la intervenció de la persona, a un nombre indeterminat de persones físiques".*

En conseqüència, el RGPD exigeix del responsable una configuració per defecte dels tractaments que siga respectuosa amb els principis de protecció de dades, advocant per un processament mínimament intrusiu: mínima quantitat de dades personals, mínima extensió del tractament, mínim termini de conservació i mínima accessibilitat a dades personals. Tot això, a més, sense que siga necessària la intervenció de l'interessat per a garantir que estos mínims estan establits.

"La PbD es fonamenta en la construcció de la privacitat com el mode d'operació predeterminat dins del model de negoci de les organitzacions i que s'estén als sistemes de tecnologies de la informació que suporten el tractament de les dades, els processos i les pràctiques de negoci relacionades i el disseny físic i lògic dels canals de comunicació utilitzats".

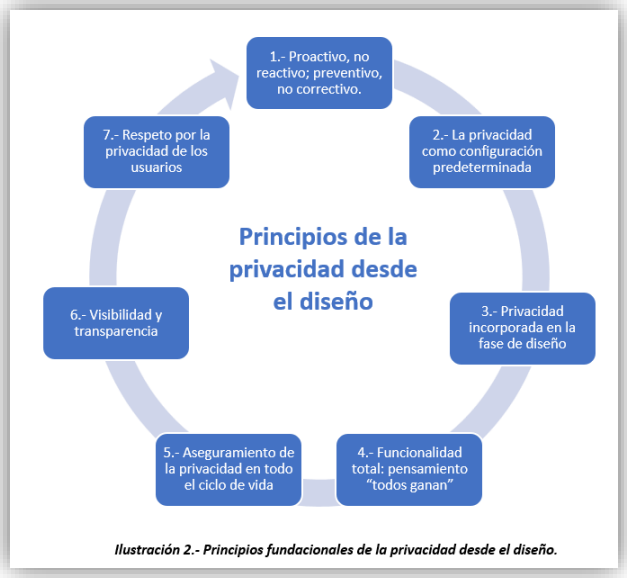


Ilustración 2.- Principios fundacionales de la privacidad desde el diseño.

2. PRINCIPIS FUNDACIONALS DE LA PRIVACITAT DES DEL DISSENY

Els següents principis van ser establits per Ann Cavoukian, durant els anys 90's, per a atendre els efectes sempre creixents i sistemàtics de les Tecnologies de la Informació i les Comunicacions, i dels sistemes de dades en xarxa a gran escala.

1.- Proactiu, no reactiu; preventiu, no correctiu. Per exemple, el desenvolupament d'una cultura de compromís i millora contínua per part de tots els treballadors així com la definició i assignació de responsabilitats concretes, de manera que cada membre de l'entitat pública sàpia clarament quines són les seues funcions en matèria de privacitat.

2.- La privacitat com a configuració predeterminada. En este supòsit, restringir els accessos a les dades personals segons les seues funcions a les parts implicades en els tractaments de dades.

3.- Privacitat incorporada en la fase de disseny. És un requisit necessari en el cicle de vida de sistemes i serveis, així com en el disseny dels processos de l'organització que siga present la privacitat.

4.- Funcionalitat total: pensament *"tots guanyen".* Si la solució tecnològica proposada a l'administració planteja amenaces a la privacitat, buscar noves alternatives per a aconseguir lus interesses perseguits sense perdre de vista els riscos per a la privacitat de l'usuari.

5.- Assegurament de la privacitat en tot el cicle de vida. Per exemple, la destrucció segura i garantida de la informació al final del seu cicle de vida

6.- Visibilitat i transparència. És important desenvolupar i publicar clàusules d'informació concises, clares i intel·ligibles, que siguen fàcilment accessibles i que permeten als interessats comprendre l'abast del tractament de les seues dades.

7.- Respecte per la privacitat dels usuaris. És destacat implementar mecanismes eficients i efectius que permeten als interessats l'exercici dels seus drets en matèria de protecció de dades.

"Les dimensions de seguretat tradicionals; confidencialitat, integritat i disponibilitat no són suficients per a garantir la privacitat per disseny, i per tant, han d'incloure's tres nous objectius que garantisquen els principis en protecció de dades. Estos objectius de privacitat són: la desvinculació, la transparència i el control".

3. OBJECTIUS DE SEGURETAT DE LA PRIVACITAT DES DEL DISSENY

Tradicionalment, el disseny de sistemes segurs i de confiança s'ha centrat en analitzar els riscos i donar resposta a les amenaces que afecten els objectius de la seguretat que estan més orientats a la privacitat: la **confidencialitat,** evitant els accessos no autoritzats als sistemes. La **integritat,** protegint-los de modificacions no autoritzades de la informació. I la **disponibilitat**, garantint que les dades i els sistemes estan disponibles quan és necessari.

No obstant això, per a donar cobertura a estos possibles riscos han d'incloure's en l'esquema d'anàlisi tres nous objectius de protecció específics de la privacitat, i la garantia de la qual es converteix en salvaguarda dels principis de tractament establits per la normativa.

- **Desvinculació *("Unlinkability"):*** Persegueix que el processament de la informació es realitze de manera que les dades personals d'un domini de tractament no puguen vincular-se amb les dades personals d'un altre domini diferent o que l'establiment d'aquesta vinculació supose un esforç desproporcionat. Els principis que pretén garantir són la minimització de dades, la limitació del termini de conservació i la integritat i confidencialitat.

- **Transparència:** Cerca aclarir el tractament de les dades de manera que la recollida, el processament i l'ús de la informació puga ser comprés i reproduït per qualsevol de les parts implicades i en qualsevol moment del tractament. Els principis que pretén garantir són la licitud, lleialtat, transparència i la limitació de la finalitat.

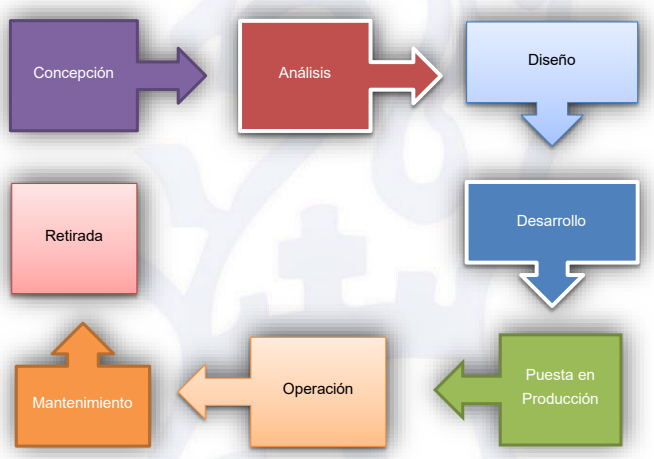
- **Control:** Garanteix la possibilitat que les parts involucrades en el tractament de les dades personals i, principalment, els subjectes les dades dels quals són tractats, poden intervindre en el tractament quan siga necessari per a aplicar mesures correctives al processament de la informació. Els principis que pretén garantir són la limitació de la finalitat, l'exactitud, la integritat, confidencialitat i la responsabilitat.

"El cicle de vida de la privacitat des del disseny consta de 8 fases: Concepción, Anàlisi, Disseny, Desenvolupament, Posada en producció, Operació, Manteniment i Retirada".

4. CICLE DE VIDA DE LA PRIVACITAT DES DEL DISSENY

La Privacitat des del Disseny pot afectar tant un sistema, com a un producte maquinari o programari, a un servei o, fins i tot, a un procés.

Siga com siga l'objecte de la PbD, comparteixen tots, el mateix cicle de vida:



Il·lustració 3.- Cicle de vida de la privacitat per disseny.

1.- Concepció: És l'etapa de planificació. En esta etapa inicial es determina l'àmbit del projecte, es realitza un estudi de viabilitat, s'analitzen els riscos associats, s'estimen els costos (assignant recursos) i es determina la duració estimada del projecte.

2.- Anàlisi: S'esbrina tots els requisits que necessita el sistema, és a dir, que funcionalitats es requereixen.

3.- Disseny: Es decideix l'estructura del sistema (l'arquitectura), definint les interfícies entre els diferents mòduls

4.- Desenvolupament: És quan s'implementa el sistema, triant el maquinari i programari necessari i que suport el sistema

"Per a complir amb la privacitat per disseny disposem de tres eines: les estratègies, els patrons de disseny i les tècniques de privacitat".

5.- Posada a producció: És l'etapa d'implementació i desplegament del sistema. Té especial importància el desenvolupament de proves, les quals pretenen detectar els errors que s'hagen comés en les etapes anteriors, per a així corregir-los.

6.- Operació: Es tradueix en la utilització del sistema per part dels usuaris en el dia a dia.

7.- Manteniment: Tot sistema ha de disposar de manteniments correctius, evolutius i perfectius.

8.- Retirada: Quan el sistema ja no ofereix utilitat i deixa d'usar-se.

5. ESTRATÈGIES, PATRONS I TÈCNIQUES DE LA PRIVACITAT

L'objectiu és que la privacitat quede integrada com a part del disseny del sistema, de manera que els requisits de privacitat siguen definits en termes de propietats i funcionalitats plenament implementables i qualsevol risc sobre la privacitat que s'haja identificat siga adequadament gestionat pel sistema de manera proactiva.

Per a això, ha de seguir-se una aproximació sistemàtica i metodològica, traslladant el quin de les fases de concepció i anàlisi (els requisits de privacitat identificats) al com de les fases de disseny i implementació (estratègies i solucions concretes) treballant, de manera seqüencial, en diferents nivells d'abstracció.

"Estratègies de privacitat: Molt al contrari, el desitjable és aplicar-les totes o el màxim possible d'elles de cara a aconseguir que l'objecte desenvolupat siga el més privacy-friendly possible".

"Patrons de disseny: Són solucions reutilitzables utilitzades per a resoldre problemes comuns i repetibles de privacitat".

Il·lustració 4.- Estratègies, Patrons i tècniques de privacitat dins del clicle de vida.

1. En el nivell més alt, en les fases inicials de concepció de l'objecte i de l'anàlisi dels seus requisits, cal treballar amb **estratègies de privacitat,** enfocaments genèrics a alt nivell dirigits a identificar aquelles tàctiques a seguir durant les diferents etapes del processament de les dades encaminades a garantir els objectius de privacitat i el compliment dels principis de tractament. Les estratègies de privacitat serveixen de pont entre els principis de tractament imposats per la norma i la implementació de la privacitat en solucions concretes. Molt al contrari, el desitjable és aplicar-les totes o el màxim possible d'elles de cara a aconseguir que l'objecte desenvolupat siga el més privacy-friendly possible. Per exemple, el suprimir per complet les dades personals tan prompte deixen de ser rellevants assegurant-se que no és possible la seua recuperació ni tan sols de les còpies de seguretat realitzades.

2. Les estratègies de privacitat es materialitzen, a més baix nivell, en **patrons de disseny de la privacitat,** solucions reutilitzables empleades en la fase de disseny que són aplicables per a resoldre problemes comuns i repetibles de privacitat que es presenten de manera reiterada en el desenvolupament de productes i sistemes. L'objectiu dels patrons és crear catàlegs de solucions reutilitzables en el disseny de la privacitat dels sistemes i estandarditzar el procés de disseny.

"Les tecnologies de privacitat millorada (PETS) són un conjunt organitzat i coherent de solucions TIC que redueixen els riscos que afecten la privacitat, implementant les estratègies i patrons de disseny".

L'associació entre patrons i estratègies no és biunívoca, de manera que un mateix patró pot implementar i donar resposta a més d'una estratègia de privacitat, proporcionant solució a diferents problemes que es presenten al llarg de les activitats de tractament de les dades. Per exemple, **la seudonimització** que permet realitzar el tractament de dades personals de manera que no puguen atribuir-se a un subjecte de dades específic sense l'ús d'informació addicional, sempre que aquesta informació addicional es mantinga per separat i estiga subjecta a mesures tècniques i organitzatives per a garantir la no atribució

3. Finalment, en el més baix nivell, en la fase de desenvolupament, es troben **les tecnologies de privacitat millorada o PETS (*Privacy Enhancing Technologies*)** que s'utilitzen per a implementar els patrons de disseny de la privacitat amb una tecnologia concreta. La Comissió, en la seua Comunicació al Parlament Europeu i al Consell sobre el foment de la protecció de dades mitjançant les tecnologies de protecció del dret a la intimitat (PET) les defineix com *"un sistema coherent de mesures de TIC que protegeix el dret a la intimitat suprimint o reduint les dades personals o evitant el tractament innecessari o indesitjat de dades personals, sense menyscapte de la funcionalitat del sistema d'informació".* Igual que ocorria amb els patrons i les estratègies de disseny de la privacitat, una mateixa solució PET pot implementar diverses solucions de patrons de disseny. Alguns tipus de PET´s estan en la següent taula:

CATEGORÍA	SUBCATEGORÍA	DESCRIPCIÓN
Protección de la privacidad	Herramientas para seudonimizar	Permiten efectuar transacciones sin solicitar información personal
	Productos y servicios para anonimizar	Proporcionan el acceso a servicios sin requerir la identificación del sujeto de datos
	Herramientas de cifrado	Protegen los documentos y transacciones de ser visualizados por terceras partes
	Filtros y bloqueadores	Evitan emails y contenido web no deseado
	Supresores de seguimiento	Eliminan las trazas electrónicas de la actividad digital del usuario
Gestión de la privacidad	Herramientas de información	Crean y verifican las políticas de privacidad
	Herramientas administrativas	Gestionan la identidad y los permisos del usuario

Il-lustració 5.- Classificacions de les PET´s

"El compliment del principi de protecció de dades per defectes ha de ser un dels elements a auditar en tota auditoria de compliment del RGPD."

6. PRIVACITAT PER DEFECTE

La configuració *'per defecte'* d'aplicacions, productes i serveis és una cosa comuna en el desenvolupament i posada en producció de sistemes a l'hora de determinar el seu funcionament. En el RGPD s'ha fixat l'obligació que tenen els responsables de garantir la PDpD de les dades personals objecte de tractament en línia amb aquesta configuració *'per defecte'.*

Així mateix, *la Guia de protecció de dades per defecte de l'AEPD* destaca en l'apartat VIII que l'emplene del principi de protecció de dades per defecte ha de ser un dels elements a auditar en tota auditoria de compliment del RGPD. La guia estableix una relació no exhaustiva d'elements de control, sent un dels elements a comprovar que no s'empren *"dark patterns"* per a manipular el procés d'elecció de l'usuari o influir de forma encoberta en la seua decisió respecte a l'abast del tractament. El terme *dark patterns* **(patrons foscos)** fa referència a interfícies i implementacions d'experiència d'usuari destinades a influenciar en el comportament i les decisions de les persones en la seua interacció amb webs, apps i xarxes socials, de manera que prenguen decisions potencialment perjudicials per a la protecció de les seues dades personals.

Per a implementar les estratègies de PDpD és necessari adoptar mesures sobre: la quantitat de dades personals recollides, l'extensió del tractament, el període de conservació i l'accessibilitat de les dades. En la Guia es pot trobar una llista, amb caràcter orientatiu, d'aquelles opcions en les quals un tractament podria ser configurable per a implementar les mesures en relació amb els elements anteriors i amb qualsevol altra circumstància en el procés del tractament susceptible d'incidir en la privacitat dels usuaris.

	Opciones de configuración agrupadas por tipo de medida	Opciones que podrían ser fijadas en el tratamiento por el responsable	Opciones que podrían incluirse en el panel de privacidad	Opciones de configuración de podrían establecerse en los componentes off-the-shelf
Cantidad de datos personales				
	Operación en modo anónimo.	X	X	
	Operación sin necesidad de crear cuenta de usuario.	X	X	

Il·lustració 6. Llista orientativa de la Guia per defecte de l'AEPD.

La Privacitat per disseny i per defecte ha de ser present en tot moment en l'entitat. Les mesures a aplicar per a complir amb la privacitat han de tindre caràcter tècnic i organitzatiu així com adoptar-se abans i durant el tractament.

7. CONCLUSIONS

a) La privacitat per disseny i per defecte es troba regulada en el *considerant 78 i article 25 del RGPD, així com en l'article 28 de la LOPDGDD*. En particular, en l'apartat primer de l'article 25 la privacitat per disseny i en l'apartat segon del mateix article la privacitat per defecte.

b) De la privacitat per disseny s'extrauen cinc característiques principals: la privacitat per disseny està orienteua **a la gestió del risc** i a la **responsabilitat proactiva** així com relacionada amb els **principis de protecció de dades.** Les mesures a aplicar per a complir amb la privacitat han de tindre caràcter **tècnic i organitzatiu.** Finalment, les mesures han d'adoptar-se **abans** i durant el tractament.

c) **Els principis fundacionals de la privacitat són:** Proactiu, no reactiu; preventiu, no correctiu. La privacitat com a configuració predeterminada. La privacitat incorporada en la fase de disseny. La funcionalitat total: pensament "*tots guanyen*". L'assegurament de la privacitat en tot el cicle de vida. La visibilitat i transparència així com el respecte per la privacitat dels usuaris.

d) Les dimensions de seguretat tradicionals; **confidencialitat, integritat i disponibilitat NO** són suficients per a garantir la privacitat per disseny, i per tant, han d'incloure's tres nous objectius que garantisquen els principis en protecció de dades. Estos objectius de privacitat són: **la desvinculació, la transparència i el control.**

e) El cicle de vida de la privacitat des del disseny consta de huit fases: **Concepción, Anàlisi, Disseny, Desenvolupament, Posada en producció, Operació, Manteniment i Retirada.** La Privacitat des del Disseny pot afectar tant un sistema, com a un producte maquinari o programari, a un servei o, fins i tot, a un procés. Siga com siga l'objecte de la PbD, comparteixen tots, el mateix cicle de vida.

Seran d'utilitat les tecnologies que milloren la protecció de la privacitat (privacy enhancing technologies o PET´s), que permeten minimitzar els riscos sense perdre la funcionalitat de l'aplicació o el sistema d'informació. Per exemple: el xifratge de dades i l'anonimització.

f) Per a complir amb la privacitat per disseny disposem de tres eines: **les estratègies de disseny, els patrons de disseny i les tècniques de privacitat millorada (PETS).**

- Les *estratègies de disseny* són enfocaments genèrics a alt nivell dirigits a identificar aquelles tàctiques a seguir durant les diferents etapes del processament de les dades encaminades a garantir els objectius de privacitat i el compliment dels principis de tractament.

- Els *patrons de disseny* són solucions reutilitzables empleades en la fase de disseny que són aplicables per a resoldre problemes comuns i repetibles de privacitat que es presenten de manera reiterada en el desenvolupament de productes i sistemes

- Les *tecnologies de privacitat millorada* són un conjunt organitzat i coherent de solucions TIC que redueixen els riscos que afecten la privacitat, implementant les estratègies i patrons de disseny.

g) En el RGPD s'ha fixat l'obligació que tenen els responsables de garantir la privacitat per defecte de les dades personals objecte de tractament en línia amb la configuració *'per defecte'.* La Guia de protecció de dades per defecte de l'AEPD identifica les estratègies que han de guiar l'aplicació de la PDpD, com són l'optimització, la configurabilidad i la restricció en el tractament de dades personals per defecte. A mes, **es desenvolupen les mesures específiques** per a la implementació de la PDpD en relació amb la quantitat de dades personals recollides, l'extensió del tractament, el període de conservació i l'accessibilitat de les dades.

- Directrius 4/2019 relatives a l'article 25 Protecció de dades des del disseny i per defecte de l'Agència Espanyola de Protecció de Dades (AEPD) en este enllaç.
- Guia de Protecció de Dades per Defecte de l'AEPD en este enllaç.
- Directrius 4/2019 del Comité Europeu de Protecció de dades (*CEPD) relatives a l'article 25 Protecció de dades des del disseny i per defecte en este enllaç.
- La guia de l'Autoritat Catalana de Protecció de dades (APCAT) "*La privacitat des del disseny i la privacitat per defecte: Guia per a desenvolupadors*" en este enllaç.
- Blog de l'AEPD "Governança i protecció de dades" en este enllaç.
- Blog de l'AEPD "*Privacitat des del disseny: Computació segura multi-part, compartició additiva de secrets*" en este enllaç.
- Orientacions i garanties de l'AEPD en els procediments d'anonimització de dades personals en este enllaç.
- Blog de l'AEPD "*Dark patterns: Manipulació en els serveis d'Internet*" en este enllaç.
- Directrius 3/2022 del CEPD sobre patrons foscos en les interfícies de les plataformes de les xarxes socials: com reconéixer-los i evitar-los en este enllaç.

NOTÍCIES

Las autoritats en protecció de dades publiquen resolucions relacionades amb la privacitat per disseny i per defecte:

• **PS/00037/2020: Procediment sancionador a una comercialitzadora d'energia solar.** "Referent a això, ha de tindre's en compte que les obligacions establides en els articles 24 i 25 del RGPD no constitueixen meres obligacions formals, sinó que com assenyala l'article 24 *"el responsable aplicarà mesures tècniques i organitzatives apropiades a fi de garantir i poder demostrar que el tractament és conforme amb el present Reglament."* I l'article 25, igualment reitera que *"el responsable del tractament aplicarà, tant en el moment de determinar els mitjans de tractament com en el moment del propi tractament, mesures tècniques i organitzatives apropiades, com la seudonimització, concebudes per a aplicar de manera efectiva els principis de protecció de dades, com la minimització de dades, i integrar les garanties necessàries en el tractament, a fi de complir els requisits del present Reglament i protegir els drets dels interessats."* ***Es tracta a més d'una obligació dinàmica, cada modificació de les mesures tècniques i organitzatives deu igualment ser objecte d'una anàlisi de riscos per a determinar si aquesta modificació és apta per a aplicar de manera efectiva els principis de protecció de dades i integrar les garanties necessàries en el tractament".***

Consulta la Resolució en este enllaç.

• **Expedient núm.: PS/00677/2022:** La protecció del dret fonamental a la protecció de dades no consisteix en una mera espera "*reactiva*" al fet que puga produir-se un problema que el lesione, sinó que els responsables del tractament han de dissenyar ***("protecció de dades des del disseny")*** amb caràcter previ a l'inici del tractament, les polítiques adequades per a la protecció d'aquest dret fonamental. I això inclou tots els aspectes regulats en el RGPD, començant per les obligacions de transparència, el respecte a l'exercici dels drets establits en el Reglament, i l'establiment de totes mesures tècniques i organitzatives necessàries per a garantir el compliment d'aquesta norma. I

- Blog de l'AEPD "*Riscos per a la privacitat en iniciar sessió amb els teus comptes de xarxes socials en altres aplicacions*" en este enllaç.
- Blog de l'AEPD "*Privacitat de grup*" en este enllaç.
- Blog de l'AEPD "*Enginyeria de la Privacitat*" en este enllaç.
- Blog de l'AEPD "*Els acurtadors de URLs i la protecció de dades*" en este enllaç.
- Blog de l'AEPD "*Xifrat i Privacitat: xifratge en el RGPD*" en este enllaç.
- Blog de l'AEPD "*Xifrat i Privacitat II: El temps de vida de la dada*" en este enllaç.
- Blog de l'AEPD "*Xifrat i Privacitat III: Xifratge Homomòrfic*" en este enllaç.
- Future of Privacy Forum "*Report Unlocking Data Protection by Design & by Default: Lessons from the Enforcement of Article 25 GDPR*" en este enllaç.

així mateix les mesures de seguretat. I tot això ha d'estar planificat i implementat amb caràcter previ a l'inici del tractament pel responsable.

• **Procediment núm.: PS/00142/2019 -** *El reclamat no ha perfilat ni ha analitzat les necessitats reals d'accés a la informació dels regidors en l'accés a les dades amb les funcions concretes de control especifique que li atribueix la normativa. Hauria d'haver limitat els accessos generals a la base de dades de gestió d'expedients dels regidors, atés que no cal el contacte permanent amb aquestes dades i accessos, i haver-se establit així per defecte en el sistema. L'establiment d'estes mesures s'encamina a la salvaguarda dels drets individuals, sent doncs la seua òptica diferent de la infracció del principi e establit en l'article 5.1.f del RGPD. Existeix com s'acredita en el present suposat l'accés a una base de gestió d'expedients amb el risc d'ús interessat per tercers, així doncs, en el moment en què s'inicia el tractament s'han de considerar els temes de protecció de dades i l'adopció de mesures que s'adeqüen al que s'estableix en estos principis de tractament de dades per defecte, considerant a més que és una entitat pública, i deduint-se que els accessos a l'aplicació continuen en l'actualitat.*

IMPOSAR a l'AJUNTAMENT D´ÁLORA, amb NIF P2901200B, per una infracció de l'article 25 2 del RGPD, de conformitat amb l'article 83.5 a) del RGPD, una sanció de prevenció.