PÍNDOLA 37. GUIA DE PROTECCIÓ DE DADES PER DEFECTE

En aquesta píndola es fa un resum de la **Guia de Protecció de Dades per Defecte** publicada per l'Agència Espanyola de Protecció de Dades (AEPD), que ofereix una visió pràctica per ajudar a aplicar aquest principi als tractaments de dades seguint el que estableix el Reglament General de Protecció de dades (RGPD) i les directrius adoptades pel Comitè Europeu de Protecció de dades.

El concepte de privacitat per defecte es refereix al fet que només **han de ser objecte de tractament les dades personals que siguin estrictament necessàries i suficients per a cada una de les finalitats del tractament**. Per això, sense importar el conjunt de dades recollides pel responsable, aquest ha de segmentar l'ús del conjunt de dades entre els diferents tractaments i entre les diferents fases dels tractaments, de manera que no totes les operacions realitzades en el marc d'un tractament s'executin sobre totes les dades, sinó que actuïn només sobre aquells que siguin necessaris i en els moments en què sigui estrictament necessari.

L'RGPD exigeix al responsable una configuració per defecte dels tractaments que sigui respectuosa amb els principis de Protecció de Dades per Defecte (en endavant, PDpD), 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.

A continuació s'enumeren breument les mesures a seguir per aplicar la PDpD. L'execució d'aquestes es centra en les estratègies **d'optimització, configuració i restricció:**

1. Optimització del tractament

L'objectiu de l'optimització és analitzar el tractament des del punt de vista de la protecció de dades, la qual cosa suposa aplicar mesures amb relació a la quantitat de dades recollides, l'extensió del tractament així com la seva conservació i l'accessibilitat. S'ha de realitzar portant a terme les següents activitats:

a) *Descomposició i anàlisis del tractament en fases*

Identificar les operacions que pugin formar part del tractament (recollida de dades, organització, registre, utilització, extracció, difusió, consulta, modificació, supressió, etc) i la relació entre elles. Després definir les activitats del tractament estructurades en fases que implementin les operacions identificades al principi, determinant la pertinença i necessitat de realitzar totes i cada una de les diverses fases que s'hagin identificat aplicant el principi de minimització.

b) *Definició de casos d'ús*

Depenent del tipus de servei que es presti als usuaris serà necessari processar una distinta extensió de dades personals. Un exemple podrien ser els diferents casos d'ús d'una aplicació bancària segons la funcionalitat desitjada per l'usuari final (gestió del compte -> mitjançant identificació, pagaments -> a través d'una interfície de pagaments, localitzador d'oficines -> utilitzant la posició actual, recepció d'ofertes per proximitat -> emprant la geolocalització continuada de l'interessat, etc). En cap cas es podrà denegar l'accés a un servei simplement perquè l'usuari opti per una configuració restrictiva amb relació a la quantitat de dades tractades.

c) *Estudi de la relació entre tractaments fets per un mateix responsable*

El responsable ha d'analitzar cada tractament en el context de l'organització per identificar les necessitats de configuració sobre els serveis comuns compartits entre diferents tractaments amb l'objectiu de, en cada tractament; determinar les dades mínimes necessàries, realitzar una separació lògica i/o física

de dades personals utilitzades, gestionar els drets d'accés i establir un espai independent pels tractaments de dades sensibles.

d) Adaptació del tractament

És necessari estudiar cada una de les fases o etapes del tractament, per a cada un dels casos d'ús definits pel responsable, i determinar:

- La necessitat de cada fase, de cara a determinar si es evitable des del punt de visat del tractament de dades personals.
- La minimització aplicable tenint en compte:
  - El conjunt mínim de dades personals que han de ser tractades en cada fase i siguin estrictament necessàries per les operacions específiques a les que donen suport.
  - La necessitat de les dades inferies, si les hagués.
  - Si la fase pot ser implementada sense utilitzar dades de caràcter personal.
- El període de conservació durant el que és necessari retenir les dades personals.
- Els criteris d'accés per aplicacions, serveis i persones:
  - Quins rols definits per l'entitat han de tenir determinats privilegis d'accés i a quines dades.
  - Quins rols externs a l'entitat s'han definit i amb quins privilegis d'accés i a quines dades.
- La capacitat de control que es donarà a l'usuari sobre les opcions anteriors.

2. Configuració

La segona estratègia és la configuració de serveis, sistemes o aplicacions, que ha de permetre l'establiment de paràmetres o opcions que determinin la forma en què es du a terme el tractament, i que siguin susceptibles de ser modificades pel responsable i fins i tot per l'usuari.

a) Configuració del tractament

La configuració del tractament per defecte té quatre aspectes que condicionen el modo de funcionament:

- La identificació dels requeriments configurables (paràmetres configurables, rangs de valors disponibles tècnicament i els valors per defectes assignats a cada paràmetre).
- Determinar quines de les opcions de configuració estaran sota control exclusiu del responsable i amb quins límits.
- En el cas de les opcions de configuració que estiguin sota control de l'usuari, determinar quines de les opcions són les considerades i amb quins límits.
- Determinar si els components predeterminats (dissenyats per altres propòsits específics) utilitzats per construir el tractament compleixen amb els requisits de configuració i s'ajustin al seu valor.

D'altra banda, per escollir la configuració per defecte s'han de determinar els següents punts:

- Els diferents casos d'ús del tractament que s'ofereixin a l'usuari en base a les finalitats perseguides.
- Les dades mínimes, en cada una de les fases i per cada un dels diferents casos d'ús identificats.
- Quins dels possibles casos d'ús disponibles es configuraran com a cas per defecte.
- Els paràmetres de configuració i els seus valors en funció del cas d'ús seleccionat per defecte.

b) *Configuració dels components*

En el cas d'utilització de components de tercers és importar determinar quins valors estan prefixats i són inalterables, quins paràmetres si són configurables i el seu valor per defecte, així com el conjunt de possibles valors que podrien prendre. També s'ha d'esbrinar si aquests components realitzen activitats de tractament innecessàries, si implementen funcionalitats addicionals i no configurables que generin efectes colaterals (comunicacions a tercers, recollida de dades de tràfic, traces d'accés, etc). En el cas de que els components estàndards no complexin amb els principis de minimització, s'haurà d'analitzar la base legitimadora del tractament i considerar la possibilitat de desactivar les funcionalitats addicionals per, arribats al cas, la eventualitat de no utilitzar-los i optar per un altre component alternatiu.

c) *Control de l'usuari*

Quan tenim un paràmetre relatiu a un tractament que és configurable s'ha de determinar si correspon donar-li control a l'usuari sobre aquesta configuració. Aquest control significa que es tingui la possibilitat de prendre decisions sobre les accions de configuració, i també implica transparència i informació sobre el resultat i conseqüències de les opcions que es poden escollir. La informació facilitada sobre les distintes funcionalitats dels casos d'ús han de fer conscients a l'usuari de quines dades seran necessàries per a que el sistema, aplicació, servei o producte pugui proporcionar i gestionar aquesta funcionalitat concreta. La utilització de casos d'ús permeten una aproximació en dos capes al control del tractament per part de l'usuari: una primera per seleccionar casos generals d'ús i l'altre per la configuració en detall de cada un d'ells.

En qualsevol cosa, si es realitza una modificació, ha de ser possible revertir el canvi als valors inicials preestablerts i recuperar la configuració original de forma senzilla, fàcil i intuïtiva.

3. Restricció per defecte

El cas d'ús que, sent el mes restrictiu per defecte, permeti accedir a la funcionalitat bàsica del sistema, ha d'estar sempre disponible i seleccionat inicialment sense necessitat de cap canvi per part del responsable o de l'usuari. També ha de complir de la forma més restrictiva possible el principi de minimització i recopilar únicament les dades estrictament necessàries per assolir el propòsit del tractament que s'ha habilitat. L'usuari haurà de modificar aquesta configuració per defecte en vol ampliar el tractament de dades personals més enllà de la base legal en la que es basa el tractament principal o si les noves funcionalitats impliquen propòsits no compatibles amb el propòsit original.

Per la seva banda, la restricció garanteix que, per defecte, el tractament sigui el més respectuós possible amb la privacitat, de manera que les opcions de configuració estiguin ajustades, per defecte, a aquells valors que limitin: la quantitat de dades recollides, l'extensió de l' tractament, la seva conservació i l'accessibilitat de les dades.

a) *Quantitat de dades*

El terme 'quantitat' implica factors qualitatius i quantitatius de les dades, per tant el responsable del tractament haurà de considerar el volum de dades personals tractat, el nivell de detall, les diferents categories, la sensibilitat i els tipus de dades personals requerits per dur a terme cada operació de tractament, incloent tant les dades recollides com les generades a partir d'aquestes.

b) *Extensió del tractament*

La implementació de la PDpD implica que les operacions de tractament sobre les dades personals realitzades pel responsable es limitaran a l'estrictament necessari per a complir amb el propòsit declarat, assegurant que les operacions que es realitzin a cada fase siguin únicament les necessàries i sobre les

dades precises, per al compliment de la finalitat de cada fase. En particular, el responsable, i quan sigui oportú l'usuari, han de poder configurar l'extensió del tractament en cada fase en funció dels casos d'ús.

c) *Període de conservació*

Les limitacions al període de conservació estan vinculades amb l'extensió del tractament. El principi de minimització estableix que si una dada personal no es necessita després d'executar-se una fase del tractament, la dada ha de ser suprimida (bloquejada o anonimitzada en alguns casos). Qualsevol retenció posterior haurà de ser objectivament justificada i fonamentada.

d) *Accessibilitat de les dades*

El grau d'accessibilitat a les dades ha d'establir-se basant-se en un anàlisis de necessitat per complir amb el propòsit del tractament, que s'implementarà mitjançant:

- Una definició de rols i responsabilitats dels membres de la organització.
- Una política de control de privilegis d'accés com a part de les mesures organitzatives.
- La incorporació de mecanismes de control d'accés a la informació tant de la part organitzativa com de la part tècnica.

Conclusions

La PDpD és una de les mesures de responsabilitat proactiva que s'integra amb la resta de les garanties establertes en el Reglament, que permet optar per diferents aproximacions i alternatives a l'hora d'implementar aquest principi. Així mateix, posa de manifest que tant els responsables de tractament de dades personals, com els encarregats i desenvolupadors, han de tenir presents les mesures de PDpD en la mesura de les seves obligacions.

Aquesta mesura ha d'aplicar-se sempre que es produeixi un tractament de dades personals independentment de la naturalesa d'aquest. L'establiment de mesures de privacitat per defecte no es deriva del resultat d'una anàlisi de riscos per als drets i llibertats, sinó que són mesures i garanties que cal establir en tot cas.

Ens panells de privacitat pels usuaris hauran de facilitar la configuració oferint una aproximació en dos nivells a través dels casos d'ús i opcions de configuració específica. A demés, la informació a l'usuari sobre la conseqüència de les seves eleccions ha de ser completa i transparent.

L'aplicació de la PDpD ha de ser demostrable, això implica que la implementació ha de ser justificada, documentada i ser auditable (per exemple utilitzant certificacions).

Per a més informació:

- https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf
- https://www.aepd.es/media/guias/PDpD-listado-medidas.xlsx

Per qualsevol dubte o aclariment addicional podeu adreçar-vos al DPD de Salut:

dpd@ticsalutsocial.cat

https://ticsalutsocial.cat/oficina-dpd/

Tel.: 93 553 26 42 (9:00 a 14:00 h.) – *TEMPORALMENT INACTIU*