UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

jornada serveisTIC UPC

Jornada TIC 2024

DADES AL PODER

Dimarts 12 de novembre a les 9:45 hores

Sala d'actes Edifici Vèrtex,
Aules Vèrtex (Campus Nord)
i xat de YouTube al canal de l'Àrea TIC

#jornadaTICUPC

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

12:15 - 13:00 Sessions Paral·leles

Sala 2 - Protecció de dades des del disseny i per defecte (Aula VS202)

Cristina Guzmán
Delegada de Protecció de Dades - Àrea Serveis Jurídics UPC

12/11/2024

Índex

I. Regulació

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'aquestes dades i pel qual es deroga la Directiva 95/46/CE (RGPD)

(78) La protecció dels drets i les llibertats de les persones físiques pel que fa al tractament de dades personals exigeix que s'adoptin les mesures tècniques i organitzatives adequades amb la finalitat de garantir que es compleixen els requisits d'aquest Reglament. Per tal de poder demostrar la conformitat amb aquest Reglament, el responsable del tractament ha d'adoptar polítiques internes i aplicar mesures que compleixin en particular els principis de protecció de dades des del disseny i per defecte. Aquestes mesures poden consistir, entre d'altres, a reduir al màxim el tractament de dades personals, seudonimitzar al més aviat possible les dades personals, donar transparència a les funcions i el tractament de dades personals, permetre als interessats supervisar el tractament de dades i al responsable del tractament, crear i millorar elements de seguretat. Cal encoratjar els productors de les aplicacions, dels productes i dels serveis basats en el tractament de dades personals perquè tinguin en compte el dret a la protecció de dades quan els desenvolupen, dissenyen, seleccionen i usen i que s'assegurin amb la deguda atenció a l'estat de la tècnica, que els responsables i els encarregats del tractament estan en condicions de complir les seves obligacions en matèria de protecció de dades. Els principis de la protecció de dades des del disseny i per defecte també s'han de tenir en compte en el context dels contractes públics.

I. Regulació

Des del **DISSENY**

Per **DEFECTE**

Article 25 RGPD. **Protecció de dades des del disseny i per defecte (PDDD)**

1. Tenint en compte l'estat de la tècnica, el cost de l'aplicació i la naturalesa, l'àmbit, el context i les finalitats del tractament, així com els riscos de probabilitat i de gravetat diversa que comporta el tractament per als drets i les llibertats de les persones físiques, el responsable **ha d'aplicar**, tant en el moment de determinar els mitjans de tractament com en el moment del tractament mateix, **mesures tècniques i organitzatives adequades**, com la seudonimització, concebudes per 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 d'aquest Reglament i de protegir els drets dels interessats.

2. El responsable del tractament **ha d'aplicar les mesures tècniques i organitzatives adequades** amb la intenció de garantir que, per defecte, únicament es tracten les dades personals necessàries per a cadascuna de les finalitats específiques del tractament.
Aquesta obligació s'aplica a la quantitat de dades personals recollides, a l'abast del tractament, al termini de conservació i a l'accessibilitat de les dades. Aquestes mesures han de garantir en particular que, per defecte, les dades personals no siguin accessibles, sense la intervenció de la persona, a un nombre indeterminat de persones físiques.

3. Es pot utilitzar un mecanisme de certificació aprovat d'acord a l'article 42, com a element per acreditar el compliment de les obligacions establertes als apartats 1 i 2 d'aquest article.

II. En resum:

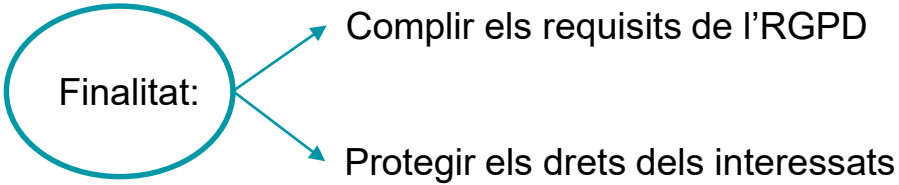
PROTECCIÓ DE DADES DES DEL DISSENY I PER DEFECTE (PDDD):

Aplicar mesures tècniques i organitzatives apropiades

Per aplicar de forma efectiva els principis de protecció de dades

+

Integrar les garanties necessàries en el tractament



L'aplicació de la PDDD ha de ser demostrable

↓

la seva implementació ha d'estar justificada, documentada i ser auditable

III. PRINCIPIS RGPD

PRINCIPIS relatius al tractament:

- Licitud, lleialtat i transparència
- Limitació de la finalitat
- Minimització de dades
- Exactitud
- Limitació del termini de conservació
- Integritat i confidencialitat
- Responsabilitat proactiva

Protecció de dades des del disseny i per defecte

IV. Des del DISSENY (PdD)

- "*l'estat de la tècnica*": el nivell tecnològic d'un servei, tecnologia o producte que existeix en el mercat i que és més eficaç per a aconseguir els objectius marcats. (concepte dinàmic)

-*s'ha d'avaluar de manera continua en el context del progrés tecnològic*-

- "*el cost de l'aplicació*": a l'hora d'escollir i aplicar les mesures tècniques i organitzatives adequades i les garanties necessàries que assegurin l'aplicació dels principis RGPD.
- "*la naturalesa*": les característiques intrínseques del tractament.
- "*l'àmbit*": grandària i varietat d'activitats del tractament.
- *"el context"*: a les circumstàncies del tractament.
- "*les finalitats del tractament*": els objectius del tractament
- "*els riscos de probabilitat i de gravetat diversa que comporta el tractament per als drets i les llibertats de les persones físiques*"

IV. Des del DISSENY (PbD)

Quan?

- En el moment de determinar els mitjans de tractament (disseny, arquitectura, procediments, protocols, la disposició i l'aparença).

- Una vegada iniciat el tractament, aplicar els principis de forma efectiva i continuada a fi de protegir els drets.

(per exemple: mantenir-se al dia de l'estat de la tècnica, reavaluar el nivell de risc, etc.)

Obligació permanent de mantenir el PbD

IV. Des del DISSENY (PdD)

Principis fundacionals de la privacitat des del disseny:

1. Proactiu, no reactiu; Preventiu, no correctiu
2. La privacitat com a configuració predeterminada
3. Privacitat incorporada en la fase de disseny
4. Funcionalitat total: pensament “tots guanyen”
5. Assegurament de la privacitat en tot el cicle de vida
6. Visibilitat i transparència
7. Enfocament centrat en el subjecte de les dades

IV. Des del DISSENY (PdD)

La PdD implica utilitzar un enfocament metodològic orientat a la gestió del risc i de responsabilitat proactiva que permeti fixar els requisits de privacitat mitjançant pràctiques, procediments i eines. Per a això:

1. A partir de l'anàlisi de risc s'establiran tant els objectius específics de protecció de dades (desvinculació, transparència i control) com els objectius de seguretat des de la perspectiva de la privacitat (confidencialitat, disponibilitat i integritat), que garanteixin els principis bàsics establerts en l'article 5 de l'RGPD.
2. A continuació, s'estudiaran les estratègies de privacitat en les quals es concreten els requisits de cada objectiu de privacitat, tant les orientades a les dades com als processos. Aquestes estratègies són: 'minimitzar', 'ocultar', 'separar', 'abstreure', 'informar', 'controlar', 'complir' i 'demostrar'; i per a cadascuna d'elles s'identificaran les tàctiques de protecció que les implementin de manera efectiva.
3. En la fase de disseny, s'integraran les tàctiques seleccionades mitjançant solucions ja conegudes, és a dir, els patrons de disseny de la privacitat, que aborden problemes comuns i repetibles, accedint als catàlegs disponibles, dels quals una selecció es presenta en aquest document.
4. En la fase de desenvolupament, es realitzarà la implementació concreta d'aquests patrons. Aquesta implementació es realitzarà per l'equip de desenvolupament bé programant en codi la funcionalitat necessària o, si és possible, fent ús de solucions TIC ja existents, és a dir, utilitzant Privacy Enhancing Technologies.

V. Per DEFECTE (PDpD)

L'RGPD exigeix del responsable una configuració per defecte dels tractaments que sigui 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.

L'establiment d'uns mínims "per defecte" → ha d'aplicar-se SEMPRE que tingui lloc un tractament de dades personals independentment de la naturalesa del tractament que es realitzi

V. Per DEFECTE (PDpD)

Best practices on data protection by default (ENISA):

Criterion 1: Minimum amount of personal data

- *The less data, the better*
- *Granular collection of data on the basis of necessity*
- *Use of privacy enhancing technologies*
- *Different minimum per purpose*
- *Minimizing the risk*
- *Considering all copies and types of data*

Criterion 2: Minimum extent of the processing of the personal data

- *The less processing, the better*
- *User empowering tools*

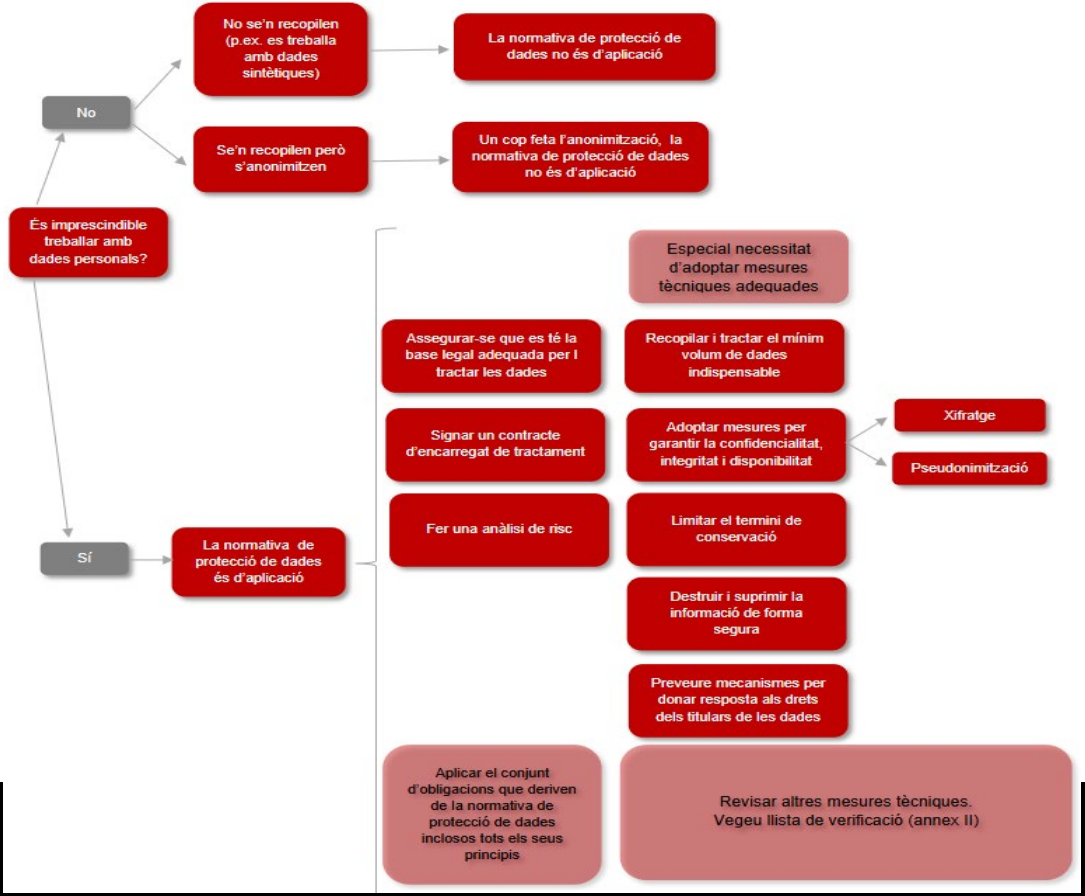
Criterion 3: Minimum period of the storage of the personal data

- *Storage – the shorter, the better*

Criterion 4: Minimum accessibility of the personal data

- *Restricting access on the basis of necessity*
- *Limiting ways of sharing*
- *No public by default without active intervention*

Anàlisi prèvia APDCAT:



VI. MESURES TÈCNIQUES I ORGANITZATIVES:

Transparència de la informació, comunicació i modalitats de l'exercici dels drets de l'interessat

PSEUDONIMITZACIÓ

Seguretat del tractament

PRIVACY ENHANCING TECHNOLOGIES (PETS) - conjunt organitzat i coherent de solucions TIC que redueixen els riscos que afecten la privacitat

ANONIMITZACIÓ

Classificació de PETS (AEPD):

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

Tabla 5 – Una de las posibles clasificaciones de las PETs (*META Group Report*)

PLA DE GESTIÓ DE DADES (PGD) / DATA MANAGEMENT PLAN (DMP):

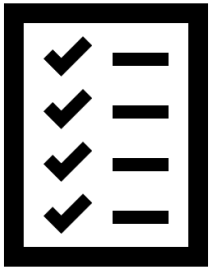
AVALUACIÓ D'IMPACTE EN MATÈRIA DE PROTECCIÓ DE DADES (AIPD):

Quan sigui PROVABLE que un tipus de tractament

COMPORTI

ALT RISC

Drets i llibertats de les persones físiques



Llista de tipus de tractaments de dades que requereixen AIPD

VII. Conseqüències

Que passa si no establim mesures tècniques i organitzatives de PDDD?

- Article 83.4.a RGPD:

"*Les infraccions de les disposicions següents se sancionen, d'acord amb l'apartat 2, amb multes administratives de 10.000.000 d'euros com a màxim o, en el cas d'una empresa, d'una quantia equivalent al 2%, com a màxim, del volum de negoci total anual global de l'exercici financer anterior, i entre les dues opcions, s'ha d'optar per la de més quantia:*

a) Les obligacions del responsable i de l'encarregat, d'acord amb els articles 8, 11, 25 a 39, 42 i 43."

- Article 73.d) i e) LOPDGDD (infracció greu):

"*d) La falta d'adopció de les mesures tècniques i organitzatives que siguin apropiades per aplicar de manera efectiva els principis de protecció de dades des del disseny, així com la no integració de les garanties necessàries en el tractament, en els termes que exigeix l'article 25 del Reglament (UE) 2016/679.*"

"*e) La falta d'adopció de les mesures tècniques i organitzatives que siguin apropiades per garantir que, per defecte, només es tracten les dades personals necessàries per a cadascuna de les finalitats específiques del tractament, de conformitat amb el que exigeix l'article 25.2 del Reglament (UE) 2016/679.*"

CASOS REALS (manca d'adopció de les mesures adequades):

Procediment sancionador núm. PS 68/2023
(informació que apareix en un justificant de visita mèdica)

Procediment sancionador núm. PS 29/2023
(compartició amb tot el professorat, de tots els cursos, la informació relativa a tot l'alumnat de l'IES a través de Google Drive)

VIII. Casos reals i guies

GUIES:

- ✔ La privacitat des del disseny i la privacitat per defecte (juny 2024) - Autoritat Catalana de Protecció de dades (APDCAT)

- ✔ Guía de Protección de Datos por Defecto (octubre 2020)
- ✔ Guía de Privacidad desde el Diseño (octubre 20219)

  Agencia Española de Protección de datos (AEPD)

- ✔ Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto (octubre 2020) - European Data Protection Board (EDPD)

- ✔ Recommendations on shaping technology according to GDPR provisions. Exploring the notion of data protection by default (desembre 2018) - European Union Agency For Network and Information Security (ENISA)

IX. Conclusions

- La PDDD és una mesura de responsabilitat proactiva.
- La PDDD s'ha d'integrar amb la resta de garanties establertes en l'RGPD.
- L'aplicació de la PDDD ha de ser demostrable, la qual cosa implica que la seva implementació ha d'estar justificada, documentada i ser auditable.
- Prendre la PbD en consideració com més aviat millor.
- Assegurar la privacitat i establir un marc de governança que garanteixi la protecció de les dades personals no representa un obstacle per a la innovació.