EAPC - Gestió de la informació: transparència i protecció de dades

La privacitat des del disseny i la privacitat per defecte: guia per a desenvolupadors de l'APDCAT

25-06-2024

En l'era digital actual, és imprescindible garantir la privacitat en tot moment per tal de protegir els drets humans que es relacionen amb la protecció de dades. Aconseguir-ho depèn de molts factors, però el més essencial és garantir que el producte o servei digital compleixi des del seu origen la privacitat des del disseny i la privacitat per defecte (art. 25 del RGPD). Això és fonamental per desenvolupar solucions tecnològiques responsables i en conformitat amb les normatives de protecció de dades. Per això, els desenvolupadors han de prioritzar la privacitat des del primer moment del procés de desenvolupament integrant pràctiques i tecnologies que protegeixin les dades dels usuaris de manera efectiva. No obstant això, la responsabilitat última recau en els responsables del tractament de dades i les entitats propietàries del producte o servei, els quals han de garantir que es mantinguin els estàndards de privacitat establerts i s'implementin les mesures adequades per protegir les dades personals dels usuaris.

Precisament, l'Autoritat Catalana de Protecció de Dades (APDCAT) té publicada la guia La privacitat des del disseny i la privacitat per defecte, adreçada a desenvolupadors i responsables del tractament en el procés de desenvolupament de noves aplicacions i serveis TIC que inclouen el tractament de dades personals, per facilitar-los l'aplicació correcta dels requeriments legals sobre protecció de la privacitat.

El concepte de privacitat des del disseny i per defecte

El concepte de la privacitat des del disseny, desenvolupat des de finals dels anys noranta pel Comissionat de Protecció de Dades d'Ontario, fa referència a la necessitat de tenir en compte l'impacte en termes de privacitat dels productes o serveis, especialment els tecnològics, ja des de la fase de disseny. Complementari a aquest, la privacitat per defecte implica l'aplicació de mesures tècniques i organitzatives adequades per assegurar que només es tracten les dades personals necessàries per a les finalitats específiques del tractament, sense necessitat d'acció per part de l'usuari.

L'article 25 del RGPD exigeix que, des del disseny d'un servei o aplicació, s'implementin mesures tècniques i organitzatives per garantir la protecció de dades personals. A més, les mesures de privacitat per defecte asseguren que les dades recollides, l'abast del tractament, el termini de conservació i l'accessibilitat, estiguin limitats al que sigui estrictament necessari. Però més enllà de l'obligació legal, cal veure-ho com una oportunitat i un avantatge competitiu.

L'article Unlocking Data Protection By Design & By Default: Lessons from the Enforcement of Article 25 GDPR analitza les obligacions legals ressaltant les dificultats en la seva implementació derivades d'una redacció ambigua i de la manca d'estàndards tècnics específics. A més, argumenta que la tecnologia garant de la privacitat (*privacy enhancing technology*, PET) és útil però no suficient per garantir plenament el compliment de les obligacions de protecció de dades des del disseny i per defecte. Conclou que una estratègia més efectiva consisteix a combinar la PET amb mètodes d'enginyeria de privacitat i a assegurar l'adequació a les directrius reguladores.

Una guia per a desenvolupadors de l'APDCAT

La guia de l'APDCAT s'ha creat per ajudar els desenvolupadors i responsables del tractament a identificar elements clau per a la protecció de dades personals i a implementar les mesures necessàries des del disseny i per defecte de les seves aplicacions. Aquesta guia ofereix consells per acompanyar els desenvolupadors en les diverses fases del cicle de vida del producte o servei, des del disseny fins al manteniment, i proporciona tècniques i estratègies per incorporar la privacitat en cada etapa del procés. A continuació, es detallen alguns dels punts clau per a cada una d'aquestes fases.

- 1. Fase de disseny
  - Minimitzar la recollida de dades
  - Amagar dades amb criptografia i control d'accés
  - Separar les dades en compartiments estancs
  - Agregar les dades sempre que sigui possible
  - Informar adequadament les persones sobre el tractament de les seves dades
  - Permetre que les persones controlin el tractament de les seves dades
  - Assegurar el compliment de les polítiques de privacitat
  - Demostrar que el tractament de dades és respectuós amb la privacitat
- 2. Fase de desenvolupament i proves
  - Separar adequadament els entorns de producció i de desenvolupament i proves
  - Allotjar la informació en llocs amb garanties adequades
  - Revisar la qualitat del codi seguint les guies de programació segura
  - Fer una anàlisi de riscos per determinar les mesures de seguretat necessàries
- 3. Recollida de dades
  - Recollir només les dades essencials
  - Valorar l'anonimització o pseudonimització de les dades recollides
  - Assegurar que el consentiment, si cal, sigui vàlid i revocable
  - Conservar evidències del consentiment obtingut
- 4. Ús de les dades
  - Classificar adequadament la informació segons les finalitats de tractament
  - Facilitar l'exercici dels drets dels usuaris
- 5. Comunicació o divulgació de dades
  - Incloure xifratge d'extrem a extrem en les comunicacions

    - Utilitzar protocols HTTPS per a serveis web
    - Aplicar sistemes d'aprenentatge federat en models d'intel·ligència artificial
- **6. Manteniment i conservació de dades**
    - Configurar un temps d'espera (*time-out*) de sessió i esborrar la memòria cau
    - Fer proves periòdiques per comprovar vulnerabilitats
    - Configurar l'execució de còpies de seguretat
    - Establir mecanismes de detecció automàtica d'intrusions i fuites d'informació
    - Limitar el període de conservació de les dades.

Recomanacions de la guia

Abans de començar qualsevol desenvolupament de productes o serveis TIC, cal determinar si és essencial treballar amb dades personals. Si no ho és, es recomana utilitzar dades sintètiques o anonimitzades, ja que les normes de protecció de dades no s'apliquen a aquestes dades. Si és necessari treballar amb dades personals, es recomana adoptar mesures tècniques adequades: recollir i processar com menys dades millor; garantir la confidencialitat, la integritat i la disponibilitat de les dades; limitar el període d'emmagatzematge; destruir i esborrar la informació de manera segura, i preveure mecanismes per respondre als drets dels subjectes de dades.

Per assegurar la protecció de dades personals al llarg del desenvolupament, és essencial tenir un llista de control de recomanacions que permeti incorporar la privacitat i la protecció de dades en cada una de les fases. A continuació, es descriuen algunes de les recomanacions que ofereix la guia:

- **1. Disseny**: Introduir estratègies i patrons de privacitat, tenint en compte les **PET** des de l'inici.

Les tecnologies garants de la privacitat (PET) són eines i mètodes dissenyats per protegir la privacitat i la seguretat de les dades personals, i ajuden a complir els requisits legals del RGPD. En la guia de l'APDCAT es comenten diversos aspectes de les PET, i l'ICO ha publicat una guia detallada per als delegats de protecció de dades i responsables de protecció de dades, que proporciona una visió clara dels beneficis i els riscos associats a aquestes tecnologies i destaca com poden ajudar a assolir la conformitat amb les lleis de protecció de dades.

- **2. Desenvolupament i proves**: signar contractes de tractament, separar entorns de producció i proves, minimitzar i anonimitzar dades, garantir la seguretat de la ubicació i la qualitat del codi, fer anàlisis de riscos i formar el personal; per exemple en DevSecOps per utilitzar-la com a metodologia de treball.

***DevSecOps* juntament amb el RGPD: una metodologia recomanada**

La integració de pràctiques de seguretat i privacitat *DevSecOps* amb el compliment del RGPD és una metodologia eficaç per garantir la protecció de dades des del disseny i durant tot el cicle de vida del desenvolupament de programari. Aquest enfocament promou la col·laboració entre equips de desenvolupament, seguretat i privacitat, i assegura que les preocupacions de privacitat s'aborden de manera proactiva en cada fase del procés.

- **3. Recollida de dades**: recollir només les dades imprescindibles, valorar l'anonimització, informar adequadament i evitar patrons foscos (*dark paterns*). Un patró fosc és una interfície d'usuari que ha estat dissenyada acuradament per enganyar els usuaris a fer coses.
- **4. Ús de les dades**: classificar la informació i facilitar l'exercici de drets.

- **5. Comunicació**: establir mecanismes de privacitat, controls d'accés, xifratge i ús de protocols segurs.
- **6. Manteniment i conservació**: establir polítiques de permisos, garantir la seguretat de les claus d'accés, fer auditories i proves de vulnerabilitat, configurar còpies de seguretat i mecanismes de recuperació, limitar el termini de conservació, aplicar l'anonimització per a fins estadístics, destruir suports no utilitzats i gestionar galetes d'una manera adequada.

Albert Serra Pagès

Coordinador de Tecnologia i Seguretat de la Informació de l'Autoritat Catalana de Protecció de Dades