DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

QUADERNS DIVALDATA

Quaderns dirigits a delegats,

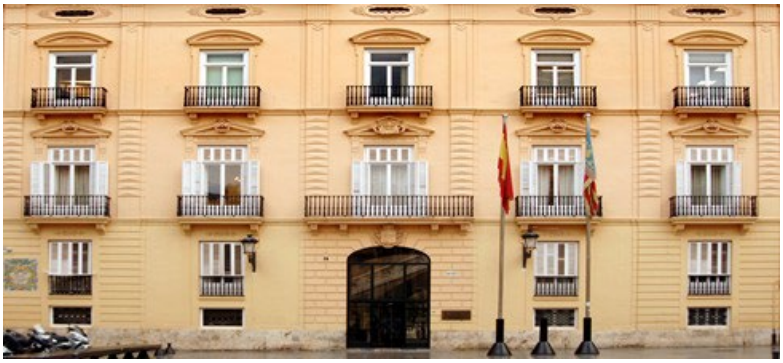
responsables i especialistes en protecció

. . . .

Quadern nº 29 | Novembre 2022

DARK PATTERNS (PATRONS FOSCOS): BONES PRÀCTIQUES

Í N D E X



DARK PATTERNS (PATRONS FOSCOS)

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

Diputació de València

Dpt. de Protecció de Dades y Seguretat de la Informació

Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUBSCRIPCIONS

Si desitges subscriure't a la nostra publicació accedeix al següent

enllaç

INTRODUCCIÓ: ¿ QUÈ SÓN ELS *DARK PATTERNS*?

El terme *dark patterns* (patrons foscos) fa referencia 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. Això és, es tracta de pràctiques poc respectuoses que busquen manipular la interacció de les persones, com: presentar massa possibilitats als usuaris que han de prendre les decisions per a fatigar-los, apel·lar a les seues emocions per a influenciar en les seues decisions, posar-los traves perquè no puguen realitzar de manera senzilla unes certes accions, etc.

Els *dark patterns* poden presentar-se a l'usuari en operacions de tractament de diversa índole, com durant el procés de registre o alta en una web, *app* o xarxa social, en iniciar sessió o també en altres escenaris com en la configuració de les opcions de privacitat, en els bàners de *cookies*, durant el procés d'exercici de drets, en el contingut d'una comunicació informant sobre una bretxa de dades personals o fins i tot en intentar donar-se de baixa de la plataforma.

En aplicació del principi de lleialtat establit en l'article 5.1.a del RGPD, el responsable del tractament ha de garantir que no s'empren *dark patterns*, almenys, en relació amb el tractament de les seues dades personals. Altres principis de protecció de dades que juguen un paper clau en l'avaluació dels *dark patterns* són els de transparència, minimització de dades i responsabilitat proactiva quant a privacitat per defecte. En algunes ocasions també el principi de limitació de la finalitat, les condicions d'obtenció del consentiment i la transparència en la informació proporcionada per a l'exercici de drets. En tot cas, el principi de protecció de dades des del disseny i per defecte ha d'aplicar-se des del moment de concepció de les interfícies i experiències d'usuaris, abans del llançament, per a garantir els drets i llibertats

"EL TERME DARK PATTERNS (PATRONS FOSCOS) FA REFERÈNCIA 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".

fonamentals de les persones, així com el compliment de la normativa.

El present Quadern, tenint en compte les recomanacions de l'Agència Espanyola de Protecció de Dades (AEPD) i del Comité Europeu de Protecció de Dades (CEPD), tracta d'establir una relació d'elements a tindre en compte perquè en la creació i configuració de les webs, *apps* o xarxes socials de la Diputació 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.

CATEGORIES

El CEPD, en el seu document de 'Directrius 3/2022 sobre patrons foscos en les interfícies de les plataformes de xarxes socials: com reconéixer-los i evitar-los' (versió 1.0, del 14 de març de 2022), divideix els dark patterns en les següents categories:

- **SOBRECÀRREGA:** els usuaris s'enfronten a una allau/gran quantitat de sol·licituds, informació, opcions o possibilitats per a demanar-los que compartisquen més dades o permetre involuntàriament el tractament de dades personals en contra de les expectatives de l'interessat.

- **OMISSIÓ:** dissenyar la interfície o l'experiència de l'usuari d'una manera que els usuaris obliden o no pensen en tots o alguns dels aspectes de protecció de dades.

- **EMOCIÓ:** afecta l'elecció que farien els usuaris apel·lant a les seues emocions.

- **OBSTACULITZACIÓ:** entorpir o bloquejar als usuaris en el seu procés d'informar-se o administrar les seues dades fent que l'acció siga difícil o impossible d'aconseguir.

"S'HA D'ESTABLIR UNA RELACIÓ D'ELEMENTS A TINDRE EN COMPTE PERQUÈ EN LA CREACIÓ I CONFIGURACIÓ DE LES WEBS, APPS O XARXES SOCIALS DE LA DIPUTACIÓ 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".

"INFLUIR EN LES DECISIONS EN PROPORCIONAR INFORMACIÓ ESBIAIXADA A LES PERSONES POT CONSIDERAR-SE UNA PRÀCTICA DESLLEIAL".

- **INCONSISTÈNCIA:** el disseny de la interfície és inconsistent i poc clar, la qual cosa dificulta que l'usuari navegue per les diferents eines de control de protecció de dades i comprenga el propòsit del tractament.

- **ENTERBOLIR:** quan una interfície està dissenyada per a ocultar informació o eines de control de protecció de dades o deixar als usuaris insegurs sobre com es tracten les seues dades i quin tipus de control poden tindre sobre ells respecte a l'exercici dels seus drets.

BUENAS PRÁCTICAS

- No s'ha de sol·licitar als usuaris més dades personals dels necessaris per als fins del tractament.

- En cas de sol·licitar dades opcionals, no s'ha de fer de manera contínua. Si els usuaris s'han negat prèviament a facilitar una dada i la sol·licitud es repeteix, aquesta sol·licitud contínua pot influir en els usuaris perquè simplement accepten la sol·licitud de la plataforma per a finalment completar el procés.

- A més, el llenguatge utilitzat no hauria de transmetre una sensació d'urgència o sonar com un imperatiu. Si els usuaris senten aquesta obligació, encara que en realitat no siga obligatori facilitar les dades, això pot tindre un impacte en el seu "lliure albir".

- No s'han d'utilitzar paraules o imatges d'una manera que transmeten informació als usuaris en una perspectiva molt positiva, fent que els usuaris se senten bé o assegurances, o molt negativa, fent que els usuaris se senten ansiosos o culpables.

"ELS INTERESSATS HAN DE REBRE INFORMACIÓ DE MANERA CLARA PERQUÈ PUGUEN COMPRENDRE COM ES TRACTEN LES SEUES DADES PERSONALS I COM PODEN CONTROLAR-LOS. A MÉS, AQUESTA INFORMACIÓ HA DE SER ACCESSIBLE I FÀCILMENT PERCEPTIBLE PELS INTERESSATS".

- El procés de registre o ingrés de dades no ha de portar més temps del necessari. Quan els usuaris intenten activar un control relacionat amb la protecció de dades, però l'experiència de l'usuari es fa de tal manera que requereix que els usuaris completen més passos en comparació amb la quantitat de passos necessaris per a l'activació de les opcions invasives de dades, és probable que això dissuadisca als usuaris d'activar els controls de protecció de dades.

- Quan als usuaris se'ls proporciona una opció relacionada amb la protecció de dades durant el procés de registre, aquests han de poder trobar aqueixa opció més tard, mentre fan ús del servei.

- S'ha de tindre en compte el principi de protecció de dades per defecte. Quan la configuració de dades està preseleccionada, els usuaris estan subjectes a un nivell de protecció de dades específic, determinat pel responsable del tractament de manera predeterminada, en lloc de per els usuaris. Degut a aquest efecte que espenta a les persones a mantindre una opció preseleccionada, és poc probable que els usuaris les canvien, fins i tot si se'ls dona la possibilitat. Per això, en cas que una de les opcions estiguera preseleccionada, aquesta hauria de ser, per defecte, l'opció més respectuosa amb la privacitat dels usuaris.

- De conformitat amb el principi de transparència, els interessats han de rebre informació de manera clara perquè puguen comprendre com es tracten les seues dades personals i com poden controlar-los. A més, aquesta informació ha de ser accessible i fàcilment perceptible pels interessats.

- Proporcionar la informació en capes pot ajudar a presentar l'avís de privacitat amb major claredat. Tanmateix, això no hauria de dificultar innecessàriament l'exercici de funcions o drets dels usuaris. Aquests no haurien d'haver de navegar a través de diferents pàgines sense tindre disponible una visió completa i exhaustiva.

- Quan els serveis estan dirigits a xiquets, hem d'assegurar-nos que el llenguatge utilitzat, inclòs el seu to i estil, siga apropiat perquè comprenguen

fàcilment la informació proporcionada.

- L'ús d'una grandària de font xicotet o l'ús de colors que no contrasten prou com per a oferir una llegibilitat suficient (per exemple, un color de text gris tènue sobre un fons blanc) pot tindre un impacte negatiu en els usuaris, ja que el text serà menys visible i els usuaris el passaran per alt o tindran dificultats per a llegir-lo. Especialment, es dona aquest cas quan es col·loquen un o més elements cridaners al costat de la informació obligatòria relacionada amb la protecció de dades. Aquestes tècniques d'interfície han d'evitar-se, ja que enganyen els usuaris i fan que la identificació de la informació relacionada amb la protecció de les seues dades siga més lenta, ja que requereix més temps i atenció per a detectar la informació rellevant.

- La presentació de la informació ha de seguir un ordre o una jerarquia. La informació relativa a la protecció de dades que manca de jerarquia es dona quan aquesta informació apareix diverses vegades i es presenta de formes diferents. És probable que els usuaris se senten confosos per aquesta redundància i no puguen comprendre completament com es tracten les seues dades i com exercir control sobre ells.

  La falta de jerarquia també pot sorgir quan la informació donada està estructurada d'una manera que dificulta l'orientació dels usuaris, per exemple, quan la Política de Privacitat compta amb més de 70 pàgines i no es proporciona un menú de navegació o índex que permeta als usuaris accedir fàcilment a la secció que busquen.

- La redacció que es dona a la informació no ha de ser ambigua o imprecisa. En cas contrari, és probable que els usuaris no estiguen segurs del tractament que es donarà a les seues dades. Per exemple, s'han d'evitar expressions com "Les seues dades podrien usar-se per a millorar els nostres serveis". En aquest cas, l'ús del temps condicional "podria" deixa als usuaris sense saber si les seues dades s'utilitzaran o no i és probable que el terme "serveis" siga massa general per a qualificar-lo com a clar.

"LA REDACCIÓ QUE ES DÓNA A LA INFORMACIÓ NO HA DE SER AMBIGUA O IMPRECISA. EN CAS CONTRARI, ÉS PROBABLE QUE ELS USUARIS NO ESTIGUEN SEGURS DEL TRACTAMENT QUE ES DONARÀ A LES SEUES DADES. PER EXEMPLE, S'HAN D'EVITAR EXPRESSIONS COM: LES SEUES DADES PODRIEN USAR-SE PER A MILLORAR ELS NOSTRES SERVICIS".

"QUAN EN LA INTERFÍCIE S'UTILITZA UN INTERRUPTOR PER A PERMETRE QUE ELS USUARIS PROPORCIONEN O RETIREN EL SEU CONSENTIMENT PER A DETERMINADES FINALDIADES, HEM DE CERCIORAR-NOS QUE LA INFORMACIÓ VISUAL NO DONE LLOC A EQUÍVOC. AIXÒ ÉS, HA DE QUEDAR CLAR PER A L'USUARI QUAN L'INTERRUPTOR ESTÀ EN MANERA CONSENTIMENT I QUAN NO".

- En nombroses ocasions, en la interfície s'utilitza un interruptor per a permetre que els usuaris proporcionen o retiren el seu consentiment per a determinades finalitats. No obstant això, hi ha vegades que la forma en la qual estan dissenyats aqueixos interruptors no deixen clar en quina posició es troba.

La informació visual no ha de donar lloc a equívoc. Això és, ha de quedar clar per a l'usuari quan l'interruptor està en manera "consentiment" o no.

MATERIAL COMPLEMENTARI

- Directrius 3/2022 sobre patrons foscos en les interfícies de les plataformes de xarxes socials: com reconéixer-los i evitar-los (CEPD).

  Consulta aquest enllaç.

- *Dark patterns:* Manipulació en els serveis d'Internet (Blog AEPD).

  Consulta aquest enllaç.

- Guia de Protecció de Dades per Defecte (AEPD).

  Consulta aquest enllaç.

- *DARK PATTERNS I:* Els *dark patterns* com a amenaça a la privacitat dels usuaris (Blog Associació Espanyola per a la Qualitat).

  Consulta aquest enllaç.

- Els reis dels *dark patterns* en termes de privacitat: els bàners de les cookies (Blog Associació Espanyola per a la Qualitat).

  Consulta aquest enllaç.

NOTÍCIES

- **L'AEPD estrena en la seva web una secció sobre el tractament de dades en Administracions Públiques.**

  La secció dedicada als tractaments duts a terme per les Administracions Públiques té com a objectiu agrupar tots aquells recursos que es troben disponibles en la web de l'AEPD perquè puguen ser utilitzats pels responsables, i especialment, per les persones que tenen assignada la funció de delegat de protecció dades i els seus equips, facilitant així l'exercici de la seua labor. Consulta la nova secció en aquest enllaç.

L'AEPD llança una eina per a ajudar els responsables a decidir si han de notificar una bretxa de dades a l'autoritat de control.

L'Agència Espanyola de Protecció de Dades (AEPD) ha llançat l'eina 'Assessora Bretxa', que té com a objectiu ajudar els responsables de tractaments a decidir si han de notificar una bretxa de dades personals a l'autoritat de control. Aquesta eina també pot ser utilitzada per delegats de protecció de dades, encarregats de tractament o consultors per a obtindre informació adequada amb la qual assessorar els responsables. Consulta la notícia en aquest enllaç.

L'AEPD sanciona al Servei de Salut de Castella-la Manxa per enviar un email a diversos dels seus treballadors amb dades (incloses dades de salut) d'uns altres.

L'AEPD sanciona al Servei de Salut de Castella-la Manxa per enviar un email a diversos dels seus treballadors amb els seus noms, categoria professional, resultats de les proves de Covid-19, si havien patit la malaltia i si això havia comportat una baixa laboral. L'email no contenia únicament la informació relativa a cada destinatari sinó també la de tots els altres. Consulta la Resolució en aquest enllaç.