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 nº 35 | Maig 2023

RISCOS DAVANT LA COMUNICACIÓ MASSIVA DE DADES ENTRE ADMINISTRACIONS PÚBLIQUES

Í N D E X

Riscos davant la comunicació massiva de dades entre Administracions públiques

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 i 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

A conseqüència de l'actual entorn de **digitalització, interconnectivitat i interoperabilitat**, ens trobem amb tractaments de dades personals que suposen l'accés o la comunicació de grans repositoris de dades entre múltiples responsables de les Administracions Públiques.

Aquests tractaments que suposen un alt volum de dades connectades de manera permanent, obliguen a considerar uns certs **riscos** en matèria de privacitat, com les **bretxes massives de dades personals** que suposen un alt risc per als drets fonamentals

S'aborda la necessitat de gestionar tant els riscos per als **drets i llibertats dels individus** com el risc per a la pròpia **societat** o per a un grup representatiu d'aquesta, derivat del **compromís de massives quantitats de dades personals.**

Aquestes infraestructures, que no tenen per què ser molt complexes tècnicament, sí que ho solen ser organitzativament per implicar múltiples actors que poden tindre diferents esferes de responsabilitat. El nombre de punts febles, on poden ocórrer possibles fallades o errors, augmenta i de la mateixa forma s'incrementa la possibilitat de materialització d'una bretxa.

Una gestió eficaç dels riscos implica **l'actuació coordinada dels diferents implicats** en el tractament, un estudi conjunt dels diferents escenaris de bretxes massives en cas de fallada de les mesures de seguretat, i l'adopció, coherent i en l'àmbit de les diferents responsabilitats, dels procediments, tècniques de protecció de dades i mesures de seguretat específiques i adequades per a minimitzar el seu impacte sobre els drets fonamentals.

"La interconnexió de sistemes i l'establiment de canals digitals permanents fan possibles els tractaments de dades que suposen l'accés o la comunicació de grans repositoris de dades entre múltiples responsables de les Administracions Públiques".

"L'impacte per als drets i llibertats que podria tindre una bretxa de dades en aquests entorns, pel fet que poden afectar un gran volum de població, és major que la suma de l'impacte que pot tindre en cadascun dels interessats".

BRETXES MASSIVES DE DADES

Una **bretxa de dades personals** és un incident de seguretat que ocasiona la **destrucció, pèrdua o alteració accidental o il·lícita de les dades personals** tractats per un responsable, o bé la comunicació o accés no autoritzats a aquests.

Una bretxa de dades personals pot tindre una sèrie d'efectes adversos considerables en les persones, susceptibles d'ocasionar **danys i perjudicis físics, materials o immaterials;** pel que cal intentar evitar-les i en cas que succeïsquen gestionar-les adequadament, especialment quan puguen posar en risc els drets i llibertats de les persones físiques.

L'article 33 del Reglament (UE) 2016/679 General de Protecció de Dades (d'ara en avant, *RGPD) imposa als responsables d'un tractament de dades personals l'**obligació de notificar a l'autoritat de control** competent les bretxes de dades personals quan siga probable que constituïsquen un risc per als drets i llibertats de les persones.

El responsable de tractament ha de valorar el nivell de risc d'una bretxa de dades personals i notificar-la a l'autoritat de control **quan existisca tal risc, i a més quan el risc siga alt el responsable també haurà de comunicar la bretxa a les persones afectades**, conforme a l'article 34 del *RGPD.

El termini per a notificar a l'autoritat de control és de **72 hores** des que l'organització té constància de la bretxa

Els tractaments de dades personals en les Administracions Públiques (d'ara en avant, *AAPP) són cada vegada **més complexos** quant al nombre d'intervinents, mitjans tècnics i tecnologies emprades. En el cas de la interoperabilitat administrativa el nivell de risc que suposaria una bretxa de dades personals és d'un elevat impacte social **molt alt**, atés que la interconnexió d'infraestructures multiplica la probabilitat que es materialitze una amenaça. **L'impacte** per als drets i llibertats que podria tindre una bretxa de dades en aquests entorns, degut al fet

"Una bretxa de dades personals és un incident de seguretat que ocasiona la destrucció, pèrdua o alteració accidental o il·lícita de les dades personals tractats per un responsable, o bé la comunicació o accés no autoritzats a aquests".

"En el cas de la interoperabilitat administrativa el nivell de risc que suposaria una bretxa de dades personals és d'un elevat impacte social molt alt, atés que la interconnexió d'infraestructures multiplica la probabilitat que es materialitze una amenaça".

"Una correcta gestió implica establir, prèviament a la materialització d'una bretxa que afecte els drets fonamentals, les mesures i accions que s'han d'adoptar en el cas que aquesta bretxa arribe a produir-sea".

que poden afectar un **gran volum de població**, és major que la suma de l'impacte que pot tindre en cadascun dels interessats.

Les conseqüències d'una bretxa massiva de dades personals en l'àmbit de les *AAPP han de ser avaluades des d'una **doble perspectiva**: d'una banda, sobre els drets fonamentals de l'individu i, d'altra banda, per l'impacte que podria suposar per a la garantia de l'interés públic i els seus efectes sobre els drets fonamentals de la pròpia societat.

Una correcta gestió implica establir, **prèviament** a la materialització d'una bretxa que afecte els drets fonamentals, les **mesures i accions** que s'han d'adoptar en el cas que aquesta bretxa arribe a produir-se

Una gestió eficaç dels riscos implica l'**actuació coordinada** dels diferents implicats en el tractament, un **estudi** conjunt dels diferents escenaris de bretxes massives en cas de fallada de les mesures de seguretat, i l'adopció, coherent i en l'àmbit de les diferents responsabilitats, dels **procediments, tècniques de protecció de dades i mesures de seguretat específiques i adequades** per a minimitzar el seu impacte sobre els drets fonamentals.

COM GESTIONAR ELS RISCOS DAVANT UNA POSSIBLE BRETXA MASSIVA

Els **riscos**, encara que sempre siguen presents, seran **especialment considerables** en tractaments duts a terme per grans organitzacions públiques i privades que estiguen donant servei a gran part dels ciutadans, i fins i tot molt més si estan interconnectades.

Per a **estimar l'impacte** que poguera tindre una bretxa de dades personals cal plantejar-se les **conseqüències que es derivarien de la seua materialització**. Per a això, poden plantejar-se els possibles escenaris de materialització d'un compromís de les dades personals, determinar les seues conseqüències, i avaluar com afecta als drets i llibertats dels interessats, sobretot si es tracta de conseqüències irreversibles en els seus drets fonamentals.

“Per a estimar l'impacte que poguera tindre una bretxa de dades personals cal plantejar-se les conseqüències que es derivarien de la seua materialització a”.

Després de l'anàlisi, cal determinar **mesures addicionals** per a disminuir la probabilitat que succeïsca la bretxa. No obstant això, s'ha d'assumir que la **possibilitat de materialització** sempre existeix i que hi ha una probabilitat residual de materialització que no es pot eliminar, per la qual cosa cal considerar **mesures específiques per a eliminar, disminuir o revertir l'impacte** de la mateixa sobre l'interessat quan aquesta es produïsca.

Per això, cal trobar la resposta, almenys, a les següents preguntes **des del disseny del tractament i prèviament a la seua implementació**:

- Quin **impacte** personal i social pot tindre una bretxa si es materialitza.
- Quines **mesures de protecció** de dades haurien d'estar implementades a priori per a minimitzar l'impacte.
- Qué **mesures de resposta** han d'estar previstes i han d'executar-se a posteriori, una vegada produïda la bretxa..

"Siga quals siguen els rols dels intervinents, les mesures i garanties de protecció de dades han de ser implementades de manera transversal a través de la cooperació de les organitzacions que intervenen".

Siga quals siguen els **rols dels intervinents**, les mesures i **garanties** de protecció de dades han de ser **implementades de manera transversal** a través de la cooperació de les organitzacions que intervenen.

Per exemple, en una situació de comunicació de dades entre responsables de la *AAPP, les mesures i garanties hauran de ser establides tant per les entitats que comuniquen o permeten l'accés a les dades (**cedents**) com per les entitats que els reben o consulten (**destinataris**) independentment dels rols que adopten en relació amb el *RGPD.

Així mateix, el *RGPD **no requereix una simple acumulació d'accions**, sinó que reclama aquelles que de manera objectiva permeten disminuir impactes sobre drets fonamentals i/o probabilitats que es produïsquen, en particular, aquelles orientades a la gestió de les bretxes de dades personals. L'acumular mesures sense saber quins problemes solucionen, com interactuen entre si i quina és la seua efectivitat real, a més de no gestionar els riscos, pot crear **vulnerabilitats addicionals**.

Convé recordar que el **ENS** (Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat), que té per objectiu la creació de les condicions necessàries de confiança en l'ús dels mitjans electrònics, a través de mesures per a garantir la seguretat dels sistemes, les dades, les comunicacions, i els serveis electrònics, i que està alineat amb el **RGPD i** la **LOPDGDD** (Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals), aplica a sistemes d'informació de AAPP i qualsevol entitat privada que preste servei a una AAPP. Per exemple, el ENS també és d'obligat compliment per als sistemes d'informació d'entitats privades que actuen com a encarregats o subencargados del tractament de AAPP.

"Les mesures tècniques i organitzatives que s'adopten han d'estar dirigides específicament a minimitzar els riscos identificats per als drets i llibertats de les potencials bretxes de dades personals".

MESURES RECOMANADES PER L'AGÈNCIA ESPANYOLA PROTECCIÓ DE DADES

Les mesures tècniques i organitzatives que s'adopten han d'estar dirigides específicament a **minimitzar els riscos identificats** per als drets i llibertats de les potencials bretxes de dades personals.

L'AEPD proposa el següent llistat de mesures, no sent exhaustiva ni exigible íntegrament, però sí que són mesures a valorar en cada cas. A continuació, s'extrauen algunes de les més rellevants:

Mesures **preventives**:

- Disposar d'un marc de coordinació dels DPD de les entitats involucrades.
- Realitzar una anàlisi conjunta de les implicacions dels tractaments que involucren a diferents entitats.
- Disposar de polítiques de protecció de dades.
- Realitzar exercicis conjunts en el qual es plantegen escenaris de bretxes de dades.
- Categoritzar dades que en un moment donat puguen ser considerats d'especial sensibilitat.
- Identificar conjunts de dades de major impacte que no hagen de ser accessibles per mitjans exclusivament automatitzats.

Mesures de **detecció**:

- Establiment de quotes o límits de consulta per usuari/compte i també per organització, concordes a l'ús legítim d'aquests, incloent-hi el monitoratge de tals accessos.
- Gestionar de manera específica les consultes/accessos des d'IP geolocalizadas en àrees geogràfiques fora de l'àmbit de les organitzacions o no habituals, IP basades en xarxes d'anonimització o IP compromeses.

" L'AEPD proposa el següent llistat de mesures, no sent exhaustiva ni exigible íntegrament, però sí que són mesures a valorar en cada cas ".

Mesures de **resposta**:

- Disposar de plans de resposta a incidents que incloguen la gestió i ràpida resposta a bretxes de dades personals.
- Disposar de procediments que permeten que els incidents de seguretat escalen de manera ràpida tant al DPD com als cercles de decisió de l'organització.
- Establiment de canals àgils, efectius i provats de comunicació de bretxes entre les entitats intervinents.
- Procediment de notificació de bretxes de dades personals a les autoritats competents que concrete tots els aspectes fonamentals.
- Procediment i recursos per a la comunicació als afectats, que avant en cada situació com es comunicarà una bretxa massiva als interessats afectats, en quines situacions es produirà tal comunicació, mitjà per a comunicar, terminis per a protegir de manera efectiva els drets dels interessats, recomanacions per als interessats en funció dels diferents escenaris de bretxes, situacions que poden justificar el retard de la comunicació, etc.

Mesures de **supervisió y revisió**:

- Procediments establits per a determinar canvis de context en responsables i tractaments de similar naturalesa: bretxes produïdes, canvis tecnològics, novetats normatives nacionals, europees i internacionals, evolució social o política, factors geoestratègics, etc.
- Establiment de canals de comunicació efectius entre les entitats intervinents sobre els esdeveniments anteriors.
- Auditories de privacitat.

MATERIAL COMPLEMENTARIO

- Orientacions per a tractaments que impliquen comunicació de dades entre Administracions Públiques davant el risc de bretxes de dades personals de l'Agència Espanyola de Protecció de Dades. Consulta aquest enllaç.
- Gestió del risc i avaluació d'impacte en tractaments de dades personals de l'Agència Espanyola de Protecció de Dades. Consulta aquest enllaç
- Guia per a la notificació de bretxes de dades personals de l'Agència Espanyola de Protecció de Dades. Consulta aquest enllaç.

NOTÍCIES

L'AEPD publica **noves notícies** en relació a les Administracions públiques**:**

1. **L'AEPD PUBLICA PER PRIMERA VEGADA EL LLISTAT D'ADMINISTRACIONS PÚBLIQUES INCOMPLIDORES AMB ELS SEUS REQUERIMENTS**. L'objectiu d'aquesta llista es troba a garantir el dret fonamental a la protecció de dades. La llista està composta per Administracions Públiques que no compleixen amb els requeriments d'informació remesos per l'Agència, així com aquelles que no adeqüen el tractament de dades a la legalitat i no acrediten les mesures correctives imposades. Tant la falta de resposta als requeriments com no acreditar que s'han complit les mesures ordenades per a garantir la protecció de dades dels ciutadans suposen infraccions classificades com molt greus. Vid. Noticia en aquest enllaç.

2. **ORIENTACIONS PER A la REALITZACIÓ D'UNA AVALUACIÓ D'IMPACTE PER A la PROTECCIÓ DE DADES EN EL DESENVOLUPAMENT NORMATIU.** L'objectiu d'aquest document és aborda la necessitat de realitzar una avaluació d'impacte des del disseny quan la mesura legislativa implica el tractament de dades personals, aportant consells i recomanacions per a dur-la a terme. Dirigit als organismes de les Administracions Públiques que promoguen projectes normatius que impliquen tractaments de dades personals i als seus delegats de protecció de dades, el document analitza els requisits previs que cal analitzar per a saber si cal fer aqueixa avaluació d'impacte, com ha de realitzar-se en cas afirmatiu i quin aspectes que s'han de tindre en compte per a avaluar la qualitat d'aquesta. Vid. guia en aquest enllaç.