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 20 | Febrer 2022

GESTIÓ I NOTIFICACIÓ DE BRETXESDE SEGURETAT: NOVETATS I REPÀS

I N D E X

GESTIÓ I NOTIFICACIÓ DE BRETXES DE SEGURETAT: NOVETATS I REPÀS

Vos convidem a traslladar-nos les temàtiques que resulten de 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

SUSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedeix al següent

enllaç

"BRETXA ÉS EL TERME QUE UTILITZEM DE MANERA MÉS COMUNA PER A DENOMINAR LA VIOLACIÓ DE SEGURETAT QUE AFECTA DADES DE CARÀCTER PERSONAL."

INTRODUCCIÓ

El Reglament (UE) 2016/679 –Reglament General de Protecció de Dades o RGPD– tracta les "violacions de seguretat" en els seus considerants 85-88, així com en els articles 4.12, 33 i 34 del seu text.

Una "violació de seguretat de les dades personals" ve definida com "tota violació de la seguretat que ocasione la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservats o tractats d'una altra forma, o la comunicació o accés no autoritzats a aquestes dades".

La conseqüència d'aquesta violació és que el responsable del tractament no és capaç de garantir més l'observança dels principis relatius al tractament de dades personals conformement a l'article 5 del RGPD. Cal diferenciar, doncs, qualsevol altre esdeveniment relacionat amb la seguretat de la informació d'una "violació de dades personals": mentre que totes les violacions de dades personals són accidents de seguretat, no tots els accidents de seguretat són violacions de dades personals.

"Bretxa", definida per la Reial Acadèmia de la Llengua com a "escletxa per on alguna cosa comença a perdre la seua seguretat", és el terme que utilitzem de manera més comuna, també d'acord amb l'anglés *data breach*, per a denominar la violació de seguretat que afecta dades de caràcter personal.

Aquesta situació pot tindre un origen accidental o intencionat i a més pot afectar dades tractades digitalment o en format paper. Com a responsable de tractament, la Diputació de València ha d'estar preparat per a possibilitats com aquestes.

L'Agència Espanyola de Protecció de Dades (AEPD) ha publicat, al juny de 2021, una nova edició *Guia per a la gestió i notificació de bretxes de seguretat.*

"LA GUIA DE JUNY DE 2021 ACTUALITZA A L'ANTERIOR COM A INSTRUMENT D'AJUDA ALS RESPONSABLES EN EL COMPLIMENT DE LES SEUES OBLIGACIONS REFERENT A LES BRETXES DE DADES PERSONALS".

Al juny de 2018 l'AEPD va publicar la primera guia dedicada a aquest tema, que va ser un instrument pioner a la Unió Europea, destinat a ajudar a responsables i encarregats en el compliment de les seues noves obligacions referent a les bretxes de dades personals.

La guia de juny de 2021 actualitza a l'anterior com a instrument d'ajuda als responsables en el compliment de les seues obligacions referent a les bretxes de dades personals. Aquesta actualització diu aprofitar l'experiència adquirida per l'AEPD, altres Autoritats de Control i el Comité Europeu de Protecció de Dades.

El seu text ens recorda, una vegada més, que qualsevol organització que tracte dades personals es troba exposada a patir una bretxa de dades personals que puga repercutir en els drets i llibertats de les persones físiques, i per tant està obligada a preveure-les i gestionar-les adequadament.

Segons l'AEPD, el procés de gestió de bretxes se suma a les polítiques d'informació ja existents en una organització i és una part necessària per a mantindre l'activitat de qualsevol entitat. Aquest procés es constitueix en una de les mesures organitzatives més importants a l'hora de salvaguardar els drets i llibertats dels interessats a través de mesures de seguretat dels tractaments

La finalitat última de la notificació i comunicació de bretxes de dades personals és la protecció efectiva dels drets fonamentals i llibertats de les persones físiques afectades per la bretxa.

Les organitzacions que patisquen una bretxa de dades personals han de focalitzar els seus esforços a evitar i mitigar les possibles conseqüències sobre els drets fonamentals i llibertats públiques de les persones afectades.

L'INCIDENT (TÈCNIC O 'HUMÀ') HAURÀ DE SER COMUNICAT IMMEDIATAMENT AL SERVEI DE PROTECCIÓ DE DADES I SEGURETAT DE LA INFORMACIÓ DE LA DIPUTACIÓ DE VALÈNCIA.

LA GESTIÓ "DE SEMPRE" DAVANT LES BRETXES DE SEGURETAT

Una de les principals obligacions davant l'esdeveniment d'una bretxa de seguretat és la seua comunicació a l'AEPD quan es complisca una sèrie de condicions.

Cal recordar que no tots els incidents de seguretat són necessàriament bretxes de dades personals i no sols els ciberincidents poden ser bretxes de dades personals. Al seu torn, no tota acció que supose una vulneració de la normativa de protecció de dades pot ser considerada una bretxa de dades personals.

Per tant, és necessari establir un criteri per a diferenciar quan l'incident es concep com una bretxa o violació de la seguretat de les dades de caràcter personal. Per a això és necessari conéixer què ha ocorregut i de quina forma les mesures de seguretat han funcionat o pal·liat els fets per a establir si realment s'ha produït o no una violació de la seguretat de les dades.

Així, el procés de gestió i notificació d'incidents es compon de les següents fases.

FASE 1: DETECCIÓ I ALERTA

Qualsevol empleat, proveïdor o una altra persona, pot informar la Diputació de l'existència d'un incident/s que poguera/n afectar la seguretat de les dades de caràcter personal.

Si la bretxa de dades personals és detectada per l'encarregat del tractament (p. ex., el nostre proveïdor), aquest haurà de remetre al responsable (p. ex., nosaltres) tota la informació necessària perquè puga complir amb les seues obligacions dins del termini i en la forma escaient.

L'incident de seguretat haurà de ser comunicat, immediatament, a aquest Servei: **dpdssi@dival.es**

FASE 2: REGISTRE DE L'INCIDENT

Per a la correcta documentació de l'incident , incloent les decisions a prendre sobre la notificació a l'AEPD i la

"LA CONTENCIÓ DE L'INCIDENT SUPOSARÀ LA PRESA DE DECISIONS RÀPIDES I ADOPCIÓ DE MESURES, TÈCNIQUES I ORGANITZATIVES".

comunicació als afectats, seran necessaris almenys la següent informació:

- Data i hora de la detecció.
- Detecció [empleat, col·laborador, 3r de confiança, extern].
- Naturalesa de l'esdeveniment de seguretat de les dades personals.
- Descripció breu.
- Sistema afectat.
- Unitat organitzativa o unitats organitzatives potencialment afectades.

En la mesura que siga possible, i encara que siga informació imprecisa o sense verificar, per a poder avaluar la severitat de l'incident, es recollirà a més la següent informació:

- Tipus i número aproximat per categoria d'interessats afectats [menors, empleats, directius, afiliats a sindicats, etc.].
- Categories i nombre aproximat de registres de dades personals afectats [DNI, nom i cognoms, adreces, matrícules, credencials, etc.].
- Nivell de certesa dels fets coneguts: [Sense evidències / Indicis d'evidència / Evidències contrastables].

FASE 3: ACTUACIONS DE CONTENCIÓ I RECUPERACIÓ ENFRONT DELS INCIDENTS

La contenció de l'incident suposarà la presa de decisions ràpides i adopció de mesures, tècniques i organitzatives, com pot ser tancar un sistema, aïllar-lo de la xarxa, deshabilitar unes certes funcions, etc. Una vegada aplicades de les mesures, s'ha de verificar el correcte funcionament d'aquestes, confirmant la seua idoneïtat per a l'eliminació de l'incident.

S'ha de considerar també si les mesures aplicades són de caràcter temporal o si formen part d'una solució definitiva, i el sistema i/o la informació afectada ha tornat de nou de manera efectiva al seu estat original.

Solucionat l'incident o la bretxa de seguretat, i verificada l'eficàcia de les mesures adoptades, es

restablirà el servei íntegrament, confirmant el seu funcionament normal i evitant en la mesura que siga possible que succeïsquen nous incidents basats en la mateixa causa. Això serà crucial per a categoritzar amb caràcter final la severitat de l'incident de seguretat en protecció de dades personals, i poder així valorar si estem davant una bretxa de seguretat.

FASE 4: VALORACIÓ DELS INCIDENTS I BRETXES DE SEGURETAT

Un dels paràmetres més importants a l'hora d'avaluar una bretxa de dades personals és determinar amb exactitud la seua tipologia, és a dir determinar a quina dimensió/és de seguretat de les dades personals ha afectat la bretxa:

- Afecta a la **confidencialitat** quan produeix una revelació no autoritzada o accidental de les dades personals, o el seu accés (per exemple: enviament de correu electrònic a una pluralitat de destinataris sense ús de còpia oculta);
- Afecta a la **disponibilitat** quan produeix una pèrdua d'accés accidental o no autoritzada a les dades personals, o la seua destrucció (per exemple: les anomenades situacions de "pantalles en negre");
- Afecta a la **integritat** quan produeix una alteració no autoritzada o accidental de les dades personals (per exemple, descobrir que han sigut modificats fitxers guardats).

Els factors a tindre en compte per a avaluar el risc de la bretxa són:

- Tipus de bretxa de dades personals.
- Facilitat d'identificar als interessats afectats.
- Naturalesa de la bretxa.
- Categories especials de dades personals.
- Volum de dades afectades.
- Gravetat dels danys ocasionats.
- Característiques de l'entitat responsable.
- Nombre d'interessats afectats.

RECORDA:

UN INCIDENT DE SEGURETAT QUE NO HA AFECTAT DADES PERSONALS O TRACTAMENTS DE DADES PERSONALS NO ÉS UNA BRETXA DE DADES PERSONALS, ATÉS QUE NO PODRIA PRODUIR DANYS SOBRE ELS DRETS I LLIBERTATS DE LES PERSONES FÍSIQUES LES DADES DE LES QUALS SÓN OBJECTE DEL TRACTAMENT, INDEPENDENTMENT D'ALTRES PERJUDICIS QUE PUGA PRODUIR AL RESPONSABLE O ENCARREGAT DEL TRACTAMENT.

"LA NOTIFICACIÓ A L'AEPD ES REALITZARÀ ABANS DE LES 72 HORES DES QUE S'HAJA TINGUT CONSTÀNCIA D'ELLA I UNA VEGADA S'HA VALORAT L'OBLIGACIÓ D'HAVER-LA DE QUE FER PELS RISCOS QUE SUPOSA".

FASE 5: NOTIFICACIONS

El responsable de tractament ha de valorar la severitat o gravetat d'impacte d'una bretxa per als drets i llibertats dels afectats en relació amb la probabilitat de produir-se, i notificar en el seu cas a l'AEPD quan es donen les condicions estipulades. En molts casos, el responsable també haurà de comunicar la bretxa a les pròpies persones afectades (sense termini concret, però "sense dilació indeguda").

La notificació a l'AEPD es realitzarà abans de les 72 hores des que s'haja tingut constància d'ella i una vegada s'ha valorat l'obligació d'haver-la de que fer pels riscos que suposa.

FASES FINALS

L'assumpte estarà en **seguiment** fins a constatar que la bretxa ha sigut definitivament resolta i que el risc per als afectats no ha sigut eliminat o reduït a nivells de risc residual acceptable. Tot seguit, es tractarà de traure **lliçons apreses**: solucionar possibles deficiències en la gestió d'incidents o incorporar millores que permeten una millor resposta en les següents execucions.

LES NOVETATS QUE PORTA LA GUIA EDITADA EN 2021

El motiu principal de l'actualització de la Guia consisteix a facilitar i agilitar el procediment de gestió i notificació de les bretxes de seguretat per part dels responsables i encarregats del tractament.

En la nova Guia s'inclou informació més específica per a la gestió integral d'una bretxa de seguretat de dades personals de manera més eficaç i eficient, els procediments obligatoris de gestió de la bretxa de seguretat i els canals de notificació davant l'Autoritat competent.

"NOTIFICAR DINS DEL TERMINI I EN LA FORMA ESCAIENTÉS UNA EVIDÈNCIA DE LA DILIGÈNCIA DE L'ORGANITZACIÓ".

SOBRE LES NOTIFICACIONS

Les notificacions de bretxes de dades personals a l'AEPD s'han de realitzar de manera electrònica, usant el formulari de notificació de bretxes de dades personals de la Seu Electrònica amb el que es pretén garantir una correcta execució de les obligacions de l'article 33.3 del RGPD.

La notificació a l'autoritat de control d'una bretxa que afecta dades personals forma part de la responsabilitat proactiva establida en el RGPD, i el fet de notificar-la no implica necessàriament l'obertura d'un procediment administratiu. De fet, notificar dins del termini i en la forma escaient és una evidència de la diligència de l'organització, mentre que no complir amb aqueixa obligació si està tipificat com a infracció.

Una vegada notificada una bretxa de dades personals a l'Autoritat de Control, el responsable de tractament ha d'estar preparat per a rebre i atendre els possibles requeriments, ordres o comunicacions que l'AEPD puga realitzar-li electrònicament en relació amb la bretxa de dades personals notificada. Per exemple:

- **Comunicació** amb informació relativa al registre de la bretxa de dades personals notificada.
- **Notificació** amb un requeriment d'informació addicional sobre la bretxa de dades personals o el tractament de dades personals en qüestió.
- Notificació amb una **ordre per a comunicar als afectats** la bretxa de dades personals en virtut de l'article 34.4 en considerar que el risc per als afectats és alt.

L'AEPD remetria les seues comunicacions i/o notificacions a l'Adreça Electrònica Habilitada (DEH) de la Diputació de València, com a entitat responsable de tractament identificada en el formulari de notificació.

Quant a les comunicacions als interessats, que hauran de realitzar-se en el seu cas –amb el contingut mínim establit en l'art. 34 del RGPD– de manera directa als

"S'INCLOU UN LLISTAT DE MOTIUS DE DEMORA EN LA NOTIFICACIÓ EN EL TERMINI ORDINARI, QUE EN QUALSEVOL CAS HAURAN D'ACOMPANYAR-SE DE L'OPORTUNA JUSTIFICACIÓ EN EL MOMENT DE LA NOTIFICACIÓ".

afectats, es recull que poden ser per mitjà de telèfon, correu electrònic, SMS, correu postal, o a través de qualsevol altre mitjà dirigit a l'afectat que el responsable considere adequat.

SOBRE ELS TERMINIS

Es tracta d'una de les principals novetats en comparació amb la versió anterior és quant als terminis.

Si bé es manté el termini de 72 hores per a notificar la bretxa de dades personals que constituïsca un risc per als drets i llibertats dels interessats, en aquesta versió s'inclou un llistat de motius de demora en la notificació en el termini ordinari, que en qualsevol cas hauran d'acompanyar-se de l'oportuna justificació en el moment de la notificació, a saber:

- el termini de 72 hores expira fora de l'horari de la jornada laboral, dia inhàbil o període de vacances;
- incidència tècnica;
- inicialment no es va considerar necessari notificar la bretxa de seguretat;
- demora en el procés de gestió; o
- interferència en una investigació policial o judicial en curs.

A més, s'estableix un màxim de 30 dies per a modificar la notificació inicial, així com el termini màxim de 30 dies per a confirmar l'execució d'una ordre emesa per l'AEPD.

VALORACIÓ DE LES BRETXES

La nova Guia reitera, en un llenguatge clar i senzill, els criteris a tindre en compte a l'hora de determinar la procedència o no de la notificació de la bretxa i, en el seu cas, la comunicació als propis afectats.

Si bé, es tracta d'una valoració que es realitzaria des del Servei de Protecció de Dades i Seguretat de la informació, amb les dades que poden ser facilitats amb tota la urgència que requereix aquestes situacions.

MATERIAL COMPLEMENTARI

- Guia per a la Gestió i Notificació de Bretxes de Dades Personals (AEPD). Consulta aquest enllaç.
- *Guidelines 01/2021 on Examples regarding Data Breach Notification* (EDPB). Consulta en aquest enllaç.
- Eina Comunica-Bretxa RGPD (AEPD). Consulta aquest enllaç.
- "Bretxes de seguretat: comunicació als interessats" (AEPD). Consulta aquest enllaç.
- Consultes freqüents (FAQS) de la Seu Electrònica de la AEPD. Consulta aquest enllaç.

NOTÍCIES

- **Les 5 claus per a navegar segur en el Dia Europeu de la Protecció de Dades.**

  Què fer per a evitar una bretxa de dades en una indústria assolada per aquest problema?

  Consulta els consells en aquest enllaç.

- **Exposar dades en grups de WhatsApp, fins i tot amb permisos previs, és il·legal.**

  Un ajuntament ha sigut sancionat per crear un grup de 'desconeguts' i no garantir la confidencialitat de dades com a mòbil, foto o nom. L'opció era implantar una llista de difusió, que és unidireccional.

  Consulta la notícia en aquest enllaç.

- **Espectacular augment de les sancions a la UE per Protecció de Dades**

  Durant 2021 l'import les multes imposades per les diferents autoritats de control europees per incompliment del Reglament General de Protecció de Dades (RGPD), ha superat els 1.000 milions d'euros, enfront dels poc més de 170 milions de 2020.

  Consulta la notícia en aquest enllaç.

- **La privacitat de les dades, un imperatiu per al 91% de les empreses espanyoles.**

  La inversió en solucions que preserven la privacitat de les dades continua creixent a mesura que les empreses veuen incrementat el seu retorn de la inversió. Preservar la privacitat ja s'ha convertit en una de les principals prioritats per al 91% de les empreses espanyoles.

  Consulta la notícia en aquest enllaç.