ACORD PEL QUE S'APROVA LA NORMATIVA PER A LA GESTIÓ DE BRETXES DE SEGURETAT DE LA UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Aprobado por Consejo de Gobierno de 25 de julio de 2024

Índex

PREÀMBUL

Amb l'entrada en vigor del 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 i la Llei orgànica 3/2018, de 5 de desembre de Protecció de Dades Personals i garantia dels drets digitals, les entitats que tracten dades personals s'han vist en l'obligació d'establir procediments i protocols per a la gestió i notificació dels incidents i bretxes de seguretat que suposen un risc per als drets i llibertats de les persones físiques.

Així les coses, la Universitat Politècnica de València (des d'ara UPV), en el desenvolupament de la normativa de seguretat ha decidit desplegar la present Normativa per a la Gestió de Bretxes de Seguretat per a la correcta gestió dels incidents que afecten dades personals la responsable de les quals és la mateixa Universitat.

L'objectiu d'aquesta normativa és desenvolupar el procediment operatiu per la Universitat en relació amb la gestió i notificació de tots els esdeveniments relacionats amb privacitat. Per això, es constitueix, a partir de la data d'aprovació, una normativa interna de compliment obligatori per a tot el personal de la UPV.

De manera general, i per a alinear la UPV amb la legislació (article 33 del RGPD), el temps màxim de comunicació a l'autoritat de control (Agència Espanyola de Protecció de Dades, a Espanya) d'una violació de privacitat no ha de superar les 72 hores des del moment en què s'identifica la violació de privacitat. Aquesta notificació l'ha de dur a terme el delegat de protecció de dades nomenat a la Universitat.

En el present procediment es regulen aspectes fonamentals de la gestió de bretxes de seguretat, com ara: (i) l'àmbit d'aplicació del procediment, (ii) la identificació i el registre inicial dels esdeveniments, (iii) la catalogació conforme a la definició de bretxa de seguretat, (iv) la gestió i tractament del risc que representa per als drets, (v) si és el cas, la notificació de la bretxa a l'autoritat de control competent, (vi) si és el cas, la notificació de la bretxa als afectats, (vii) així com la resta d'obligacions derivades per a tots els subjectes obligats pel present procediment.

En la creació d'aquest document s'han vist implicades les principals àrees per a la gestió dels incidents i bretxes de seguretat, entre aquestes: l'Àrea Jurídica i de Delegació de Protecció de Dades, l'Àrea de Sistemes d'Informació i Comunicacions (ASIC) i, en aplicació del concepte de Top-Down per a la gestió de les polítiques de *compliance* i compliment normatiu, els més alts òrgans de direcció de la Universitat.

Article 1. Objecte

L'objectiu d'aquesta norma és definir i establir el procediment mitjançant el qual s'han d'identificar, catalogar, resoldre i/o escalar totes les entrades relacionades amb esdeveniments en què es veuen implicades dades personals.

Article 2. Definicions

1. Dades personals: qualsevol informació sobre una persona física identificada o identificable (persona interessada). S'ha de considerar persona física identificable qualsevol persona la identitat de la qual es pot determinar, directament o indirectament, en particular mitjançant un identificador, com per exemple un nom, un número d'identificació, dades de localització, un identificador en línia o un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona.

2. Tractament: qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunts de dades personals, ja siga per procediments automatitzats o no, com són la recollida, registre, organització, estructuració, conservació, adaptació o modificació, extracció, consulta, utilització, comunicació per transmissió, difusió o qualsevol altra forma d'habilitació d'accés, acarament o interconnexió, limitació, supressió o destrucció.

Article 3. Àmbit d'aplicació

Aquest document s'aplica a totes les activitats de la UPV en l'àmbit de l'obtenció, tractament i comunicació de dades de caràcter personal.

1. Aquest document és de compliment obligatori per a tota la comunitat universitària o personal extern que té accés a les dades de caràcter personal tractades per la Universitat. Les normes internes contingudes en el present document s'han de posar en coneixement de tota la comunitat amb accés a dades de caràcter personal o amb accés als sistemes d'informació de la Universitat, perquè sàpiguen com actuar davant la detecció d'una possible bretxa de seguretat.

2. El present document s'aplica a tots els sistemes d'informació de què disposa la Universitat als diferents centres de treball, d'acord amb el que estableix l'annex I, apartat 1, de la present normativa.

Article 4. Comunicació dels incidents

1. En el moment que un usuari del sistema de la informació identifica un esdeveniment, incident o violació de seguretat, l'ha de notificar en el termini de 24 hores al delegat de protecció de dades i a la unitat d'incidents de l'ASIC en les dades indicades en l'annex I, apartat 2, de la present normativa.

2. La comunicació s'ha de realitzar per correu electrònic i cal indicar de forma detallada la situació detectada, les conseqüències que ha produït aquesta i les actuacions dutes a terme per l'usuari.

3. Per a contactar amb la unitat d'incidents, l'usuari pot utilitzar també els mitjans de contacte disponibles en l'annex I, apartat 2, de la present normativa.

Article 5. Identificació i registre inicial dels incidents de seguretat

1. La identificació d'una entrada de privacitat pot ocórrer per diversos actors diferenciats, com, per exemple: un empleat que sol·licita l'obertura d'una entrada, seguretat corporativa, Gestió de Personal, per un 3r de confiança especialitzat, etc.

2. Independentment de l'actor que identifique el cas, l'esdeveniment l'ha de registrar el personal de l'ASIC en el registre d'incidències com a incident de seguretat, que conforma el punt centralitzador de l'incident, en el qual s'incorpora la informació inicial de l'esdeveniment i es cataloga inicialment de manera homogènia. Els rols i responsabilitats en aquest sentit els designa l'ASIC en la instrucció o el document corresponents.

3. Si l'incident afecta dades personals, l'ASIC ha d'informar de manera immediata el delegat de protecció de dades i la directora de l'Àrea Jurídica i Delegació de Protecció de Dades, per a avaluar l'afectació dels drets i llibertats dels interessats i valorar la comunicació a l'Agència Espanyola de Protecció de Dades (AEPD) i als interessats.

La centralització a l'ASIC com a equip centralitzador de primer nivell permet la implicació i coordinació dels diferents departaments requerits per a resoldre cadascun dels esdeveniments de manera eficaç segons la seua naturalesa.

4. Els registres mínims per a emplenar en un incident de seguretat amb afectació a dades personals són:

a) Data i hora de la detecció.
b) Detecció [empleat, col·laborador, 3r de confiança, extern].
c) Naturalesa de l'esdeveniment de seguretat de les dades personals.
d) Descripció breu.
e) Sistema afectat.
f) Tipus i nombre aproximat per categoria d'interessats afectats [menors, empleats, directius, afiliats a sindicats, etc.].
g) Categories i nombre aproximat de registres de dades personals afectades [DNI, nom i cognoms, adreces, matrícules, credencials, etc.].
h) Descripció de les possibles conseqüències de l'esdeveniment de privacitat.
i) Descripció de les mesures adoptades per a contenir i mitigar l'esdeveniment.
j) Criticitat en relació amb privacitat [es desenvolupa en el capítol següent].
k) Estat actual de l'esdeveniment.
l) Procediment de resolució [si s'aplica].
m) Data de resolució [si s'aplica].

5. És possible que durant el primer registre de l'esdeveniment no es dispose de tota la informació descrita i, en aquest cas, s'ha de sol·licitar més informació i la investigació de l'esdeveniment per a poder emplenar almenys amb informació aproximada els camps requerits.

Article 6. Catalogació i escalat d'esdeveniments de privacitat

1. Una vegada registrada l'entrada de privacitat i recopilada la informació disponible en primera instància, es realitza una primera catalogació. Es considera bretxa de seguretat "qualsevol incident de seguretat o violació de la seguretat que ocasione la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra forma, o la comunicació o accés no autoritzat a aquestes dades", segons indica l'article 4.1 del Reglament 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.

2. S'estableixen tres grans categories per a les entrades de privacitat, a saber: esdeveniment, incident i violació. Aquesta última categoria referent a la violació de privacitat se subdivideix, així mateix, en dues categories segons l'afecció que supose a les llibertats i drets dels afectats.

3. S'entén per violació de seguretat de dades de caràcter personal qualsevol violació de la seguretat que ocasione la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra forma, o la comunicació o accés no autoritzats a aquestes dades. En tot cas, qualsevol entrada que afecte o impacte en les dimensions de la seguretat (confidencialitat, integritat o disponibilitat) s'ha de considerar almenys com un esdeveniment de privacitat, sempre que afecte un sistema d'informació que continga dades de caràcter personal.

Els criteris que ha de complir una entrada per a ser categoritzada com a tal a la Universitat es defineixen en l'annex II de la present normativa.

Article 7. Gestió i tractament d'entrades

1. Segons la classificació de l'entrada, el seguiment i tractament d'aquesta varia depenent de si ens trobem davant un esdeveniment, una incidència o una violació.

2. Per a la gestió dels *esdeveniments*, el tractament i resolució habitual de l'entrada realitzat pels procediments estàndard de l'ASIC. El responsable de seguretat reporta al delegat de protecció de dades l'existència de l'esdeveniment mitjançant un informe detallat tan prompte com tinga constància de l'afectació de dades personals.

3. Per a la gestió de les *incidències*, el tractament i resolució habitual de l'entrada realitzat pels procediments estàndard de l'ASIC . El responsable de seguretat reporta al delegat de protecció de dades l'existència de l'esdeveniment mitjançant un informe detallat tan prompte com tinga constància de l'afectació de dades personals. Tant l'ASIC com el delegat de protecció de dades poden iniciar una investigació sobre l'incident de cara a obtenir-hi més informació, de manera que es puguen adoptar les mesures de protecció addicionals que es consideren, així com la possible notificació de la incidència a l'AEPD.

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

4. Per a la gestió de les *violacions*, el tractament i resolució habitual de l'entrada realitzat pels procediments estàndard de l'ASIC. El responsable de seguretat reporta al delegat de protecció de dades l'existència de l'esdeveniment mitjançant un informe detallat tan prompte com tinga constància de l'afectació de dades personals. Tant l'ASIC com el delegat de protecció de dades poden iniciar una investigació sobre l'incident de cara a obtenir-hi més informació, de manera que es puguen adoptar les mesures de protecció addicionals que es consideren, així com la possible notificació de la incidència a l'AEPD.

Article 8. Notificació a les autoritats

1. Qualsevol entrada categoritzada com a *violació de privacitat* la notifica a l'Agència Espanyola de Protecció de Dades o autoritat de control competent el delegat de protecció de dades de la Universitat. La notificació es realitza a tot tardar 72 hores després que se n'ha tingut constància.

2. Si la incidència s'ha produït en el sistema d'informació de la Universitat, es comunica al delegat de protecció de dades en un termini màxim de 24 hores des que s'ha tingut constància de la incidència.

3. Si la incidència s'ha produït en el sistema d'informació d'un tercer, encarregat del tractament de la Universitat, aquest tercer comunica a la Universitat la incidència en un termini màxim de 24 hores des que va tenir constància i, seguidament, la Universitat ho comunica al delegat de protecció de dades en un termini de 24 h addicionals. La comunicació al delegat de protecció de dades es realitza mitjançant el canal corresponent indicat en l'annex I d'aquesta norma.

4. Així mateix, el delegat de protecció de dades de la Universitat, i sota el seu propi criteri, pot notificar les entrades catalogades com a *incident* que considere oportunes. El criteri general per a aquests casos és notificar qualsevol entrada que puga suposar un risc per als drets i les llibertats de les persones físiques.

5. En la notificació s'ha d'incloure almenys la informació següent:

a) Descriure la naturalesa de la violació de la seguretat de les dades personals, inclusivament, quan siga possible, les categories i el nombre aproximat d'interessats afectats, i les categories i el nombre aproximat de registres de dades personals afectades.
b) Comunicar el nom i les dades de contacte del delegat de protecció de dades o d'un altre punt de contacte en què es puga obtenir més informació.
c) Descriure les possibles conseqüències de la violació de la seguretat de les dades personals.
d) Descriure les mesures adoptades o proposades pel responsable del tractament per a posar remei a la violació de la seguretat de les dades personals, incloent-hi, si és el cas, les mesures adoptades per a mitigar els possibles efectes negatius.
e) En cas que no siga possible facilitar tota la informació en un primer report, es poden realitzar notificacions graduals que incorporen la informació requerida segons se'n dispose.

6. La notificació es realitza a la seu electrònica de l'Agència Espanyola de Protecció de Dades. A manera de contingència, en cas de no estar disponible el servei electrònic de l'Agència Espanyola de Protecció de Dades, s'ha de contactar amb aquesta per qualssevol dels mitjans facilitats en l'annex I d'aquesta norma, per a acordar el canal alternatiu pel qual realitzar la notificació.

Article 9. Notificació als interessats

1. Qualsevol *violació de privacitat* categoritzada com a *crítica* es notifica als afectats després de la revisió prèvia del contingut de la notificació pel delegat de protecció de dades. La notificació es realitza com més prompte millor, una vegada que s'ha tingut constància de l'abast i afectació als drets i llibertats dels interessats.

2. La notificació descriu, en un llenguatge clar i senzill, la naturalesa de la violació de privacitat i conté almenys la informació següent:

a) Nom i dades de contacte del delegat de protecció de dades o d'un altre punt de contacte en què es puga obtenir més informació.
b) Descripció de les possibles conseqüències de la violació de la seguretat de les dades personals.
c) Descripció de les mesures adoptades o proposades pel responsable del tractament per a posar remei a la violació de la seguretat de les dades personals, incloent-hi, si és el cas, les mesures adoptades per a mitigar els possibles efectes negatius.

3. S'estableixen les excepcions següents a l'obligatorietat de la comunicació de les entrades catalogades com a *violació de privacitat* definida com a *crítica* als interessats en cas de complir-se alguna de les condicions següents:

a) S'han adoptat mesures de protecció tècniques i organitzatives apropiades de manera que es pot assegurar que la informació personal és inintel·ligible per a qualsevol persona que no estiga autoritzada per a accedir a la informació (P. ex.: xifratge).
b) El responsable del tractament ha pres mesures ulteriors que garanteixen que ja no hi ha la probabilitat que es concrete l'alt risc per als drets i llibertats dels interessats.
c) Supose un esforç desproporcionat. En aquest cas, s'opta en el seu lloc per una comunicació pública o una mesura semblant per la qual s'informa de manera igualment efectiva els interessats.

Article 10. Comunicació a empleats i col·laboradors

1. Qualsevol entrada que supose una violació de privacitat catalogada com a *crítica* la notifica als empleats i col·laboradors l'ASIC, després de la revisió prèvia del contingut de la notificació pel delegat de protecció de dades.

2. La notificació descriu, en un llenguatge clar i senzill, la naturalesa de la violació de privacitat, així com el posicionament corporatiu en relació amb la violació ocorreguda.

Article 11. Contenció i mitigació

1. En cas de requerir-se la contenció i mitigació tècnica, l'entrada s'identifica addicionalment com a *ciberincident*, amb la qual cosa es gestiona el tractament segons el procediment estàndard de seguretat.

2. En cas de tractar-se d'un cas d'excepcional gravetat, es pot sol·licitar la invocació del procediment de gestió de crisi o pla de continuïtat.

Article 12. Incompliment de la Normativa

1. El responsable de seguretat de la informació, en l'exercici de les seues funcions, davant un possible incompliment de la present normativa que puga suposar un perjudici greu per a la informació o les dades personals tractats per la UPV, pot, després de l'autorització prèvia del rector, procedir a la suspensió cautelar del tractament de dades realitzat, així com al bloqueig temporal de sistemes, comptes o accessos a la xarxa de manera preventiva, amb la finalitat de garantir el bon funcionament dels serveis de la institució, sense perjudici dels procediments administratius i disciplinaris que corresponguen, si és el cas.

2. En els altres supòsits d'incompliment, s'adverteix del fet l'infractor. En cas que l'usuari no responga o ignore l'advertència, el responsable de seguretat de la informació de la Universitat pot iniciar els procediments administratius i disciplinaris que corresponguen, si és el cas.
Tot això sense perjudici d'iniciar les accions judicials civils i, si és el cas, penals que puguen correspondre, en relació amb les persones presumptament implicades en aquest incompliment.
La Universitat Politècnica de València posa en coneixement de l'autoritat judicial i les forces i cossos de seguretat de l'Estat les infraccions que poden ser constitutives de delicte.

Disposició final única. Entrada en vigor

Aquesta normativa entra en vigor el mateix dia de la publicació en el *Butlletí Oficial de la Universitat Politècnica de València* (BOUPV).

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen

ANNEX I – Dades de contacte

1. Centres de treball de la UPV:
   a) Campus de Vera, situat al Camí de Vera, s/n, CP 46022 – València (Espanya)
   b) Campus d'Alcoi, situat a la plaça de Ferrándiz i Carbonell, s/n, CP 03801 – Alcoi (Alacant-Espanya)
   c) Campus de Gandia, situat al C/ Paranimf, 1, CP 46730 – Grau de Gandia – (València - Espanya)
   d) Qualsevol altre centre de treball físic que s'establisca en el territori d'actuació de l'entitat.

2. Dades de contacte per a la comunicació dels incidents:
   a) Delegat de protecció de dades: dpd@upv.es
   b) Unitat d'incidents de l'ASIC:
   - Adreça electrònica: incidentes@upv.es.
   - Telèfon: Si l'usuari és persona externa a la comunitat, ha de telefonar al +34 96 387 77 50; i si és personal de la Universitat, ha de marcar l'extensió 77750.
   - Aplicació Gregal, disponible per a la comunitat universitària i externs.

3. Dades de contacte de l'Agència Espanyola de Protecció de Dades:
   a) Telèfons: 901 100 099 - 912 663 517
   b) Adreça postal: C/ Jorge Juan, 6. 28001 – Madrid, Espanya.

ANNEX II – Quadre de categorització dels esdeveniments de seguretat

Categoria	Criticitat RGPD	Descripció del nivell	Exemples de perjudici potencial a l'usuari
Esdeveniment	Negligible	L'impacte sobre les persones afectades és molt reduït. Els possibles inconvenients es poden esmenar fàcilment.	- Pèrdua de temps per necessitat de repetir procediments. - Pèrdua de confidencialitat d'una dada personal aïllada.
Incident	Limitat	L'impacte sobre les persones afectades està delimitat. Els possibles inconvenients es poden esmenar, encara que requereix un esforç econòmic i treball addicional.	- Perjudici econòmic menor. - Pèrdua de confidencialitat de diverses dades personals per afectat. - Perjudici social potencial menor.
Violació de privacitat	Important	L'impacte sobre les persones afectades és elevat. Els possibles inconvenients són difícilment corregibles, ja que requereixen un esforç econòmic i treball significatius.	- Compromís de dades financeres de l'usuari. - Pèrdua de confidencialitat d'un nombre significatiu de dades personals per afectat. - Pèrdua de confidencialitat de dades sensibles identificables. - Suplantació d'identitat. - Degradació de la propietat. - Pèrdua d'ocupació. - Perjudici social potencial seriós (discriminació, afecció física o psicològica).
Violació de privacitat	Crític	L'impacte sobre les persones afectades és crític. Els possibles inconvenients són molt difícilment corregibles o irremeiables.	- Risc financer, com ara grans deutes. - Pèrdua de confidencialitat d'un nombre elevat de dades personals per afectat. - Suplantació d'identitat amb credencials oficials (certificats DNI-e, etc.). - Incapacitat per a treballar. - Perjudici social potencial permanent (discriminació, afecció física o psicològica).

Editor: Secretaria General / UPV · D.L.: V-5092-2006 · ISSN: 1887-2298 · www.upv.es/secgen