PROTOCOL DE NOTIFICACIÓ DE BRETXES DE SEGURETAT DE DADES PERSONALS DE LA UNIVERSITAT DE VALÈNCIA

ÍNDEX

Primer. Objecte i àmbit d'aplicació.

1. El procediment que recull aquest protocol pretén donar compliment al Reglament General de Protecció de Dades de la Unió (a partir d'ara RGPD) i a la llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia de drets digitals (LOPDGDD) en matèria de detecció i notificació de violacions o bretxes de seguretat que puguen afectar la seguretat de dades de caràcter personal incorporades a tractaments que siguen responsabilitat de la Universitat de València, independentment del format o suport en el qual estiguen emmagatzemades o organitzades.

2. Així mateix té per objecte donar compliment a les obligacions relatives a la gestió, resposta i documentació-registre intern d'incidents de seguretat. Una vegada detectada la bretxa de seguretat, en funció de la seua naturalesa i abast, la Universitat de València disposa d'un termini de 72 hores per a informar l'autoritat de control competent, valorar la possible notificació a l'Agència Espanyola de Protecció de Dades i, si escau, quan la bretxa de seguretat puga comportar un alt risc per als drets i les llibertats dels titulars de les dades, la comunicació als afectats.

3. Aquest procediment serà aplicable a qualsevol usuari dels sistemes d'informació de la Universitat de València quant al tractament de dades de caràcter personal, ja siga membre del personal docent investigador (PDI), ja del personal investigador en formació (PIF), ja del personal d'administració i serveis (PAS), ja siga estudiant o persona externa que es connecten i utilitzen aquests sistemes d'informació per la via de la web institucional o per accés físic a la documentació.

Segon. Bretxes de seguretat. Concepte i identificació.

1. Una bretxa és una exposició innecessària d'informació o dades de caràcter personal que pot conduir a la seua visualització, captura o manipulació per tercers no autoritzats.

El RGPD defineix d'una manera àmplia les "violacions de seguretat de les dades

personals" com: "totes les violacions de la seguretat que ocasionen 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." Solen classificar-se en les categories següents:

- Bretxa de confidencialitat: accés a la informació de qui no està autoritzat o té un propòsit il·legítim per a accedir-hi.
- Bretxa d'integritat: alteració de la informació original i substitució de dades que pot ser perjudicial per a l'individu o il·lícita.
- Bretxa de disponibilitat: impedeix l'accés a les dades originals quan és necessari. Pot ser temporal (les dades són recuperables, però això requerirà un període de temps, la qual cosa pot ser perjudicial per a l'individu), o permanent (les dades no poden recuperar-se).

La Universitat de València ha informat i ho fa ara sobre les mesures de seguretat que s'han d'adoptar a títol individual.

https://www.uv.es/ensuv/es/uvstic-seguridad-tecnologias-informacion-comunicaciones.html

Òbviament, aquest tipus de bretxes de seguretat individuals han de ser comunicades al DPD i tractades si afecten dades de la UV, si bé el protocol s'aplica també a tots els fitxers i tractaments de dades institucionals de la UV.

2. Identificació. Els casos més comuns de possible violació de dades personals són:

- **Accés a dades no autoritzat:**
  - Encàrrec del tractament sense el contracte corresponent.
  - Accés indiscriminat a impressores, fotocopiadores, etc.
  - Accés a informació confidencial no autoritzat: nòmines, currículums, embargaments, videovigilància, etc.
  - Accés no autoritzat als sistemes informàtics**.**

• Comunicació no autoritzada de dades:

- Transmissió il·lícita de dades a un destinatari. Error en l'adreça de correu.
- Vulneració del secret professional.
- Publicació d'imatges sense autorització de l'interessat.
- Enviament de correus electrònics massius sense ocultar els destinataris (còpia oculta).
- Transferència internacional de dades sense estar subjecta a una decisió sobre l'adequació de la UE o garanties adequades de protecció de dades.

• Alteració de dades:

- Modificació de dades malintencionada.
- Falsificació de dades.
- Recuperació ineficaç de còpies de seguretat.

• Pèrdua d'informació:.

- Extraviament o oblit de suports (portàtil, llapissera de dades o disc extern)
- Robatori o sostracció d'informació (portàtil, llapissera de dades o disc extern)
- Desinstal·lació d'aplicacions informàtiques.
- Per causes del transport.
- Reorganització de l'empresa.

• Destrucció de dades:

- No usar destructora de paper o de suports digitals.
- Incendi, inundació o altres causes alienes a l'empresa.

- **En qualsevol dels casos esmentats anteriorment pot haver-hi violacions de dades per falta de mesures de seguretat:.**

    - Antivirus, “antispam”, “antimalware”, “antiransomware”, “Firewall”, xifratge, seudonimització, etc.
    - Identificació i autenticació per a accedir als sistemes informàtics.
    - Mecanismes de seguretat per a accedir al mobiliari o a departaments amb dades personals.
    - Disposició de dades a la vista dels qui no estan autoritzats (recepció, monitors, taules, etc.).

Tercer. Pla d’actuació.

1. Detectada i identificada una bretxa de seguretat per qualsevol usuari dels sistemes d’informació de la Universitat de València, és necessari comunicar-ho internament a l’efecte de la seua anàlisi, classificació, elaboració d’un pla de resposta amb el disseny de les mesures que calga adoptar per contenir, reduir o eliminar possibles danys i, si escau, iniciar la notificació. No fer-ho és una infracció greu o lleu d’acord amb la LOPDGDD.

2. A aquest efecte, davant de qualsevol detecció d’exposició de dades personals, bé siga en llocs que incloguen suports físics o informàtics, l’usuari haurà d’emplenar el formulari de l’annex II donant el major nombre de detalls necessaris per a la seua anàlisi i valoració, i enviar-lo per correu electrònic a l’Oficina de Protecció de Dades de la Universitat de València (lopd@uv.es), sense perjudici que per determinades circumstàncies o per motius d’urgència es puga comunicar telefònicament al número 661 85 45 02 (delegat per ala protecció de dades de la Universitat de València i les seues fundacions).

3. El delegat per a la protecció de dades analitzarà la comunicació per determinar si es tracta d’una bretxa de seguretat relacionada amb la protecció de dades de caràcter personal.

4. Si ho és, el delegat per a la de protecció de dades, amb l'ajuda del Servei d'Informàtica, determinarà les mesures correctores i els controls que calguen, que comunicarà als responsables dels tractaments afectats.

5. El delegat per a la protecció de dades recollirà les dades necessàries per comunicar-ho a l'Agència de Protecció de Dades en el termini màxim de 72 hores des de la detecció i, si escau, als interessats afectats.

Quart. Inscripció d'incidents en el Registre de Bretxes de Seguretat de Dades Personals de la Universitat de València.

1. Davant de qualsevol incident, el delegat per a la protecció de dades obrirà un expedient de seguretat de la informació en l'aplicació creada per tractar aquests incidents i l'anotarà com a "exposició d'informació", així mateix donarà d'alta l'expedient en el Registre de Bretxes de Seguretat de Dades Personals.

2. El Registre de Bretxes de Seguretat de Dades Personals, custodiat pel delegat per a la protecció de dades, comptarà amb la següent informació sobre cada incident de seguretat de dades de caràcter personal:

A. Tipus de notificació (núm. registre, data i tipus).

B. Dades del delegat per a la protecció de dades.

C. Dades del responsable del tractament.

D. Dades de l'encarregat del tractament (si n'hi ha).

E. Informació temporal sobre la bretxa (data de detecció, mitjans de detecció, justificació de notificació tardana, data d'inici de la bretxa, estat de resolució) .

F. Sobre la bretxa:

a. Resum de l'incident.

b. Tipologia (confidencialitat, integritat o disponibilitat).

c. Mitjà pel qual es va materialitzar la bretxa.

d. Context.

e. Mesures preventives aplicades abans de la bretxa.

G. Sobre les dades afectades:

a. Categoria de les dades.

b. Categories especials de dades.

c. Nombre aproximat de registres de dades afectats.

H. Sobre els subjectes afectats (perfil i nombre dels afectats).

I. Possibles conseqüències:

a. En bretxa de confidencialitat.

b. En bretxa d'integritat.

c. En bretxa de disponibilitat.

d. Naturalesa de l'impacte potencial sobre els subjectes.

e. Severitat de les conseqüències per als individus.

f. Mesures preses per solucionar la bretxa i minimitzar l'impacte amb els afectats.

J. Comunicació als interessats (si es comunica: data, nombre de subjectes informats, mitjà utilitzat, justificació per a no informar).

K. Implicacions transfrontereres.

L. Dades relatives a incidència interna (número, data, denunciant)

2. En tot cas, la violació o bretxa de seguretat quedarà reflectida en els pertinents registres

d'activitats de tractament addicionals i complementaris que es duguen de cada fitxer o tractament**.**

Cinquè. Organització de la gestió i comunicació de bretxes de seguretat de dades personals.

- Responsable de la informació: delegat per a la protecció de dades.

- Responsable de l'àrea de seguretat informàtica de la UV i SIUV: anàlisi i, si escau, comunicació de la bretxa, així com obertura, si es creu convenient d'un expedient amb el Centre Criptològic Nacional (CCN).

ANNEX I

Marc legal

Europeu:

- 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 (reglament general de protecció de dades), (articles 33 i 34).

Nacional

- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (art. 73).

- Reial decret 3/2010, de 8 de gener, modificat pel Reial decret 951/2015, pel qual es regula l'esquema nacional de seguretat en l'àmbit de l'administració electrònica.

Sectorial

- Política de seguretat de la informació de la Universitat de València aprovada per la Junta de Govern de la Universitat de València.

- Reglament de seguretat de la informació de la Universitat de València aprovada per la Junta de Govern de la Universitat de València.

ANNEX II

FORMULARI PER A NOTIFICACIÓ DE BRETXES DE SEGURETAT (per a enviar a lopd@uv.es)

Denunciant o notificador. -

DNI/NIE/PASSAPORT:	**Nom i cognoms**
Telèfon de contacte:	**Correu-e:**
Unitat/servei/dpt. al qual està adscrit en laUV :	

Informació temporal sobre la bretxa. -

Data de detecció de la bretxa:

Mitjans o forma com s'ha detectat la bretxa:

_____

_____

Resum de l'incident:

_____

_____

_____

_____

_____

_____

Nombre aproximat de possibles afectats:

Altres detalls i circumstàncies:

_____

València, ... d ... de 20...

Signat:

ANNEX III

Registre d'activitats de tractament sobre bretxes de seguretat

INFORMACIÓ BÀSICA SOBRE PROTECCIÓ DE LES DADES PERSONALS QUE HA DONAT	
Responsable:	UNIVERSITAT DE VALÈNCIA
Legitimació:	El tractament és necessari per al compliment d'una obligació legal aplicable al responsable del tractament (art. 6.1.c *Reglament general de protecció de dades*).
Finalitat:	Detecció, control i resposta a les bretxes de seguretat en la Universitat de València, i notificació, si escau, a l'autoritat de control i als interessats.
Destinataris:	Delegat per a la protecció de dades i Servei d'Informàtica de la Universitat de València.
Drets:	Pot sol·licitar l'accés, oposició, rectificació, supressió o limitació del tractament de les seues dades, tal com s'indica en la informació addicional.
Informació addicional:	Pot consultar la informació addicional i detallada sobre protecció de dades en: https://www.uv.es/uvweb/universitat/ca/universitat/delegacio-proteccio-dades-/delegacio-1286042855523.html

Així mateix, en el model de registre d'activitats de tractament específic i ampliat de cada fitxer s'han d'indicar les bretxes de seguretat que afecten cada fitxer.