UNIVERSITATEA „VALAHIA" DIN TÂRGOVIŞTE

GESTIONAREA INCIDENTELOR DE SECURITATE ÎN CADRUL UNIVERSITĂȚII VALAHIA DIN TÂRGOVIȘTE

COD: PO 06.13

PROCEDURĂ OPERAŢIONALĂ

ROMÂNIA UNIVERSITATEA VALAHIA DIN TÂRGOVIȘTE SENAT MINISTERUL EDUCAȚIEI NAȚIONALE

Aprobat Senat:

Prof. univ. dr. Constantin PEHOIU

Responsabilităţi	Prenumele şi numele	Funcţia	Semnătura	Data
Elaborat	Ec.drd. Mădălina OACHEŞU	Responsabil cu protecţia datelor din cadrul UVT (DPO)		07.11.2018
Verificat	Conf.univ.dr. Ilioara GENOIU	Coordonator Compartiment evaluarea şi asigurarea calităţii Secretar Comisie de monitorizare		22.11.2018
Avizat	Conf. univ. dr. Laura Monica GORGHIU	Prorector învăţământ şi asigurarea calităţii, Preşedinte Comisie de monitorizare		06.12.2018

EDIŢIA: **1** REVIZIA: **0** 1 2 3 4 5

Prezenta procedură a fost avizată în şedinţa Comisiei de monitorizare din data 06.12.2018 şi a fost aprobată în şedinţa Senatului universitar din data de 31.01.2019.
Prezenta procedura intră în vigoare pe data aprobării de către Senatul universitar.

1. SCOP

Procedura descrie cerințele și regulile care trebuie respectate pentru a minimiza impactul incidentelor de securitate.

2. DOMENIU DE APLICARE

2.1. Pentru gestionarea rapidă și eficientă a incidentelor de securitate a datelor cu caracter personal, în cadrul structurilor UVT va fi desemnată o echipă/mai multe echipe de gestionare a incidentelor de securitate formată/formate din personalul responsabil de acțiunile desfășurate în scopul micșorării sau eliminării impactului negativ al unui incident de securitate.

2.2. Prezenta procedură se aplică în mod unitar în cadrul UVT, colectării și prelucrării datelor cu caracter personal, efectuate, în totalitate sau în parte, prin mijloace automate precum și colectării și prelucrării prin alte mijloace decât cele automate a datelor cu caracter personal care fac parte dintr-un sistem de evidență și care sunt destinate să fie incluse într-un asemenea sistem.

3. DOCUMENTE DE REFERINŢĂ

- Regulament nr. 679 din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor).
- Legea Educaţiei Naţionale nr. 1/2011, cu modificările şi completările ulterioare;
- Legea 129/2018 pentru modificarea și completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea ANSPDCP, precum și pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date.
- Legea nr. 682/2001 privind ratificarea Convenţiei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981.
- Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.
- Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului UE 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016;
- Carta Universității "Valahia" din Târgoviște.

4. DEFINIŢII ŞI ABREVIERI

4.1. Definiţii

4.1.1. Încălcarea securității datelor cu caracter personal - încălcare a securității care duce, în mod accidental sau ilegal, la ***distrugerea***, ***pierderea***, ***modificarea*** sau

divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod sau la accesul neautorizat la acestea

4.1.2. Incidente de securitate - orice pierdere, deteriorare, distrugere accidentală sau divulgare a datelor, materiale sau informaţii

4.2. Abrevieri

DPO – Responsabil cu protecţia datelor cu caracter personal
GDPR – General Data Protection Regulation
PO – procedură operaţională
UVT – Universitatea „Valahia" din Târgovişte

5. DESCRIEREA PROCEDURII

5.1. Prezenta procedură descrie cerinţele şi regulile care trebuie respectate pentru a minimiza impactul incidentelor de securitate.

5.2. Prin încălcarea securităţii datelor cu caracter personal se înţelege o încălcare a securităţii care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea.

5.2.1. Astfel:

a) ***distrugerea*** se referă la situaţia în care datele nu mai există ori nu mai există într-o formă care să le facă utilizabile de către UVT;
b) ***pierderea*** are în vedere situaţia în care datele pot să existe, însă UVT a pierdut controlul sau accesul la date;
c) ***modificarea*** desemnează situaţia în care datele sunt corupte sau modificate în alt mod, astfel încât ele nu mai sunt complete;
d) ***divulgarea neautorizată*** are în vedere situaţia în care datele au fost transmise ori accesate de către persoane neautorizate să primească sau să acceseze datele personale.

5.2.2. Exemple de incidente de securitate:

- orice pierdere, deteriorare, distrugere accidentală sau divulgare a datelor, materiale sau informaţii;
- un telefon pierdut sau furat şi/sau alt dispozitiv portabil, cum ar fi un scaner etc., sub rezerva ca acesta aparţine UVT ori este folosit în interes de serviciu;
- pierderea sau furtul laptop-urilor sau computerelor desktop pe care sunt stocate date cu caracter personal;
- probleme cu comunicaţiile electronice, cum ar fi trimiterea email-urilor care conţin informaţii cu caracter personal la adrese de e-mail greşite;
- incidente legate de apă, foc, gaze, inclusiv inundaţii, scurgeri,

disfuncționalități, alarmă sau sistem de monitorizare;
- încercări repetate de acces sau acces/utilizare neautorizat/ă a sistemelor informatice ale UVT;
- infiltrarea de viruși sau alte software-uri malițioase în sistemele informatice;
- compromiterea conturilor utilizatorilor sau a parolelor.

5.3. Descrierea procesului de tratare a incidentelor de securitate

5.3.1. Raportarea incidentelor este responsabilitatea oricărui utilizator de date cu caracter personal de a raporta apariția sau suspiciunea apariției unui incident de securitate conducătorului structurii UVT în care acesta lucrează.

5.3.2. Dacă acesta nu poate fi contactat atunci se vor contacta persoanele nominalizate de acesta.
5.3.3. Lista acestor persoane cu datele de contact este adusă la cunoștința tuturor salariaților din cadrul structurii respective.
5.3.4. Dacă niciunul dintre aceștia nu este disponibil se va lua legătura direct cu echipa de gestionare a incidentelor de securitate.
5.3.5. În momentul în care conducătorul departamentului/structurii/serviciului sau una din persoanele nominalizate în lista cu persoane de contact este anunțată de un utilizator de date cu caracter personal de apariția unui incident, acesta va verifica cele semnalate. După verificare, acesta va raporta imediat și echipei de gestionare a incidentelor furnizând totodată detaliile pe care le-a aflat. Dacă este posibil, pe baza informațiilor primite despre incident se vor dispune primele măsuri ce trebuie întreprinse pentru soluționarea incidentului.
5.3.6. După declanșarea incidentului, echipa de gestionare a incidentelor de securitate va monitoriza rezolvarea lui. Aceasta va ține legătura cu persoana care a raportat incidentul pe tot parcursul gestionării acestuia asigurând suport pentru rezolvare. Toate incidentele raportate vor fi analizate în cadrul întâlnirilor echipei/echipelor de gestionare a incidentelor de securitate.

5.4. Analiza incidentelor de securitate

5.4.1. Ulterior informării cu privire la existența unui incident de securitate, echipa de gestionare a incidentelor va proceda la analiza acestuia, urmând a stabili următoarele:
- dacă sistemele de stocare/prelucrare a datelor cu caracter personal au fost compromise și dacă au fost, de cât timp;
- identificarea sistemelor afectate sau supuse riscului de a fi afectate;
- identificarea informațiilor care au fost luate sau modificate;
- identificarea metodelor folosite pentru accesarea datelor;
- identificarea măsurilor ce trebuie întreprinse pentru stoparea incidentelor și securizarea datelor cu caracter personal;
- identificarea consecințelor unui incident de securitate asupra confidențialității și securității datelor cu caracter personal, precum și asupra capacității UVT

de a-și desfășura activitatea în condiții normale;
- estimarea timpului de remediere.

5.4.2. Estimarea perioadei de timp necesare remedierii se realizează în funcție de factori precum: resursa afectată, informațiile primite de la utilizatorul de date cu caracter personal care a raportat incidentul, capacitatea echipei de răspuns, necesitatea deplasării în teren/accesul fizic pentru soluționare/distanța până la locație, măsurile ce trebuie luate pentru remedierea incidentului, tipul și gravitatea evenimentului.

5.4.3. Echipa de gestionare a incidentelor va dispune de posibilitatea răspunsului imediat la incidente, sens în care, până la emiterea răspunsului pe termen lung la incidente, aceasta poate dispune:
- utilizarea unor soluții de back-up/alternative (de exemplu, folosirea unor spații de stocare de rezervă/alternative, recrutarea serviciilor pe canale alternative, reluarea traficului de internet);
- izolarea echipamentelor/segmentelor/sistemelor afectate;
- remedierea problemelor prin aplicarea unor măsuri/soluții (de exemplu, înlocuirea unor echipamente defecte, reconfigurarea/reinițializarea unor echipamente/sisteme software, reconfigurări de parametri, intervenția manuală, relocarea fizică);
- cooperarea cu alte părți - alți furnizori de rețele și servicii de comunicații electronice, furnizori de utilități, producători de echipamente etc.

5.4.4. În ceea ce privește acțiunile de răspuns pe termen lung la incidente de securitate a datelor cu caracter personal, echipa de gestionare a incidentelor va întreprinde:
- acțiuni de remediere/restabilire completă a sistemelor/rețelelor/serviciilor;
- implementarea unor măsuri tehnice și organizatorice pentru prevenirea altor incidente similare/actualizarea măsurilor tehnice existente (de exemplu, achiziționarea de echipamente pentru înlocuirea celor afectate, actualizarea proceselor, politicilor și procedurilor operaționale, implementarea unor soluții de back-up, schimbarea tehnologiilor/soluțiilor tehnice, contractarea unor servicii, modificări în configurația rețelei pentru minimizarea impactului unui potențial incident/redesign al soluției/platformei de rețea, îmbunătățirea mecanismelor de detectare a incidentelor, implementarea unor măsuri de securitate fizică, implementarea de noi platforme de servicii);
- analize post-incident și verificarea/monitorizarea sistemelor/rețelelor/serviciilor (de exemplu analiza post-incident care conține cauza incidentului, modul de soluționare și acțiuni post-incident pentru evitarea incidentelor de același tip, testarea preventivă a sistemelor neafectate, simulări de atacuri cibernetice, evaluarea riscurilor, urmărirea modului de funcționare a sistemelor/echipamentelor implicate pe o anumită perioadă de timp, monitorizarea

soluțiilor adoptate pentru răspunsul la incidente).

5.4.5. Gestionarea incidentelor de securitate va trebui documentată în mod corespunzător, sens în care echipa de gestionare a incidentelor va păstra o evidență a incidentelor petrecute în cadrul UVT, prin completarea unor rapoarte ce vor conține cel puțin următoarele informații:

- momentul producerii incidentului;
- cauza incidentului;
- locația incidentului;
- descrierea resurselor afectate (echipamente etc.);
- corelarea cu alte incidente/evenimente asociate (dacă este cazul);
- rezultatele analizei/evaluării incidentului, respectiv deciziile luate în vederea remedierii sale, acțiunile întreprinse în vederea remedierii incidentului, acțiunile planificate pentru recuperarea integrală în urma incidentului și pentru prevenirea altor incidente similare;
- informații de contact ale părților implicate – ale celui ce detectează/raportează incidentul și ale celui/celor ce se ocupă de tratarea acestuia;
- statusul incidentului în diferite etape/momente de timp pe tot parcursul desfășurării sale.

5.5. Notificarea Autorității de Supraveghere

5.5.1. În cazul în care are loc o încălcare a securității datelor cu caracter personal, UVT este obligată să notifice acest lucru autorității de supraveghere, fără întârzieri nejustificate, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta.

Notificarea autorității de supraveghere nu este obligatorie în cazul în care încălcarea securității datelor nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice.

5.5.2. Este obligația UVT să analizeze dacă incidentul de securitate cu care se confruntă generează riscuri pentru drepturile și libertățile persoanelor vizate. Analiza se face de la caz la caz, pe baza următoarelor elemente:

a) tipul incidentului;
b) natura, contextul, volumul datelor afectate;
c) posibilitatea de a identifica persoanele vizate;
d) consecințele incidentului asupra persoanelor vizate;
e) circumstanțele persoanelor vizate;
f) circumstanțele operatorului în cauză.

5.5.3. Conținutul minim al notificării:

(a) descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
(b) comunică numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
(c) descrie consecințele probabile ale încălcării securității datelor cu caracter personal;
(d) descrie măsurile luate sau propuse spre a fi luate de UVT pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor efecte negative.

5.5.4. Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.

5.6. Informarea persoanelor vizate

5.6.1. Informarea persoanelor vizate este obligatorie numai dacă incidentul de securitate este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor vizate. Dacă notificarea autorității de supraveghere este obligatorie ori de câte ori există un risc privind drepturile și libertățile persoanelor vizate, informarea persoanelor vizate este obligatorie atunci când există un risc **ridicat** pentru drepturile și libertățile acestora.

5.6.2. În cazurile în care informarea persoanelor vizate este obligatorie, aceasta trebuie făcută fără întârziere și va include:
(a) o descriere într-un limbaj clar și simplu a caracterului încălcării securității datelor cu caracter personal;
(b) numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
(c) o descrie a consecințelor probabile ale încălcării securității datelor cu caracter personal;
(d) o descrie a măsurilor luate sau propuse spre a fi luate de UVT pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

5.6.3. Informarea persoanei vizate nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită:
(a) UVT a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;

(b) UVT a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate nu mai este susceptibil să se materializeze;

(c) ar necesita un efort disproporționat, situație în care se efectuează o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

6. RESPONSABILITĂŢI

6.1. Rectorul:

- asigură aplicarea procedurii;
- alocă resursele necesare desfășurării procesului și aplicării procedurii;
- pe baza informațiilor primite despre incident se vor dispune primele măsuri ce trebuie întreprinse pentru soluționarea incidentului în cel mai scurt timp posibil.
- în cazul în care are loc o încălcare a securității datelor cu caracter personal, UVT este obligată să notifice acest lucru autorității de supraveghere (ANSPDCP), fără întârzieri nejustificate, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta;
- notificarea autorității de supraveghere nu este obligatorie în cazul în care încălcarea securității datelor nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice.

6.2. Responsabilul cu protecţia datelor din cadrul UVT (DPO):

- elaborează și propune modificarea/ retragerea prezentei proceduri;
- instruieşte responsabilii cu protecţia datelor din cadrul structurilor UVT şi utilizatorii autorizaţi în vederea aplicării şi respectării prezentei proceduri;
- analizează periodic activitatea responsabililor cu protecţia datelor din cadrul structurilor UVT şi a utilizatorilor autorizaţi;
- verifică respectarea prezentei proceduri;
- informează conducerea UVT despre vulnerabilităţile şi riscurile semnalate în sistemul de securitate a prelucrării datelor cu caracter personal al structurii şi propune măsuri pentru înlăturarea acestora;
- informează ordonatorul de credite în ceea ce privește cerințele și regulile care trebuie respectate pentru a minimiza impactul incidentelor de securitate;
- informează conducerea UVT în legătură cu orice încălcare a normelor de protecţie a datelor cu caracter personal de natură a prejudicia drepturile persoanei vizate, cu privire la măsurile dispuse pentru identificarea persoanei responsabile şi limitarea efectelor unei diseminări neautorizate a datelor, precum şi cu privire la situaţiile în care au fost emise recomandări sau aplicate sancţiuni de către Autoritatea Naţională de Supraveghere sau când aceasta a dispus efectuarea unui control prealabil ori a unor investigaţii;
- coordonează soluţionarea cererilor persoanelor vizate;
- ţine evidenţa cererilor persoanelor vizate.
- în cazul în care are loc o încălcare a securității datelor cu caracter personal, aduce la cunoștința conducerii UVT obligativitatea de a notifica acest lucru

autorității de supraveghere (ANSPDCP), fără întârzieri nejustificate, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta.

6.3. Decani/directori de departamente/ directori de direcţii/şefi de birou/:

- informează conducerea UVT despre vulnerabilităţile şi riscurile semnalate în sistemul de securitate a prelucrării datelor cu caracter personal al structurii şi propune măsuri pentru înlăturarea acestora;
- asigură ca responsabilul din cadrul acestor structuri să informeze în cel mai scurt timp DPO-ul în cazul în care are loc o încălcare a securităţii datelor cu caracter personal;
- în cazul în care are loc o încălcare a securităţii datelor cu caracter personal asigură prin toate mijloacele posibile furnizarea informaţiilor necesare soluționării incidentului.

6.4. Oficiul juridic:

- răspunde de actualizarea informaţiilor privind actele normative aplicabile universităţii şi de difuzarea lor către structurile interesate;
- asigură consilierea juridică în ceea ce privește legalitatea deciziilor luate.

7. ÎNREGISTRĂRI

-

8. ANEXE

-

CUPRINS