UNSTPB
27980
16/09/2024

INSTRUCȚIUNE DE LUCRU PRIVIND RECUNOAȘTEREA INCIDENTELOR DE SECURITATE A DATELOR CU CARACTER PERSONAL ȘI MODUL DE ACȚIONARE ÎN CAZUL NEDORIT AL APARIȚIEI ACESTORA ÎN UNIVERSITATEA NAȚIONALĂ DE ȘTIINȚĂ ȘI TEHNOLOGIE POLITEHNICA BUCUREȘTI

1. SCOP GENERAL

Scopul acestei instrucțiuni este de a informa și sensibiliza toate structurile din **Universitatea Națională de Știință și Tehnologie POLITEHNICA București** referitor la identificarea utilizării frauduloase, la distrugerea accidentală sau ilegală, pierderea, modificarea sau dezvăluirea neautorizată a datelor personale deținute de universitate, cât și a modului de a acționa și raporta în cazul apariției nedorite a unor astfel de incidente.

2. OBIECTIVE

Această instrucțiune de lucru are ca obiective principale:

- Să constituie un instrument în sprijinul fiecărui membru al personalului universității, în vederea recunoașterii unui eventual incident de securitate;
- Să ajute la evitarea și prevenirea utilizării/modificării/dezvăluirii frauduloase, neautorizate, ilegale, a pierderii sau a distrugerii accidentale a datelor cu caracter personal deținute de către universitate;
- Să contribuie la stabilirea unui mod de lucru transparent privind raportarea internă de către angajați a unor astfel de incidente, atât pe linie ierarhică, cât și către responsabilul cu protecția datelor din universitate;
- Să ajute la evaluarea riscului unui incident de securitate cu privire la gradul de afectare a drepturilor și libertăților persoanelor vizate;
- Să instruiască factorii de decizie din universitate privind modul de administrare a unor astfel de incidente de securitate, incluzând condițiile de raportare către *Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal* și informarea persoanei vizate.

3. DEFINIȚII

În Regulamentul GDPR (REGULAMENTUL (UE) 2016/679 - Regulamentul general privind protecția datelor) sunt prevăzute următoarele definiții, conexe acestui regulament:

3.1. „date cu caracter personal" - înseamnă orice informații privind o persoană fizică identificată sau identificabilă (denumită generic „persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

3.2. „prelucrare" - înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

3.3. „operator" - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

3.4. „persoană împuternicită de operator" - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

3.5. „parte terță" - înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism, altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

3.6. „încălcarea securității datelor cu caracter personal" - înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarca neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau accesul neautorizat la acestea;

4. CADRUL LEGAL DE REFERINȚĂ

- REGULAMENTUL (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);
- LEGE nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);
- Orientări privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679.

Inginerie și cercetare pentru viitor | Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România | E-mail: dpo@upb.ro | www.upb.ro

5. NOȚIUNI PRIVIND ÎNCĂLCAREA SECURITĂȚII DATELOR PERSONALE, ÎN CONTEXTUL GDPR

5.1.Ce înseamnă o încălcare a securității datelor personale?

O încălcare a securității datelor cu caracter personal reprezintă un incident de securitate care poate duce la distrugerea accidentală sau ilegală, pierderea, modificarea sau dezvăluirea neautorizată a datelor și poatc conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei vizate.

Următoarele acțiuni ar putea conduce către apariția unor incidente de securitate:

- Accesul ncautorizat al unei terțe părți la baze de date personale ale universității;
- Permiterea accesului unei persoane neautorizate la un echipament de calcul sau într-un spațiu unde sunt stocate date cu caracter personal;
- Divulgarea accidentală sau intenționată a unor date personale colectate/prelucrate/stocate de către universitate;
- Trimiterea de informații/fișiere, ce conțin date personale, către un destinatar greșit;
- Pierderea sau furtul unor echipamente electronice portabile (laptop, tabletă, hard-disk extern, telefon) pe care sunt stocate date cu caracter personal;
- Modificarea accidentală sau neautorizată a unor date personale deținute de universitate;
- Pierderea sau distrugerea accidentală a bazelor de date personale, fără posibilitatca reconstituirii acestora într-un termen rezonabil, în vederea respectării "dreptului de acces" al persoanei vizate;
- Publicarea pe un site web a unor date cu caracter personal fără acordul persoanei vizate;
- Pierderea posibilității de accesare a datelor personale în urma criptării frauduloase a bazelor de date, ca efect al unui atac cibernetic asupra rețelei informatice a universității.

Pe scurt, orice incident de securitate a datelor cu caracter personal afectează confidențialitatea, integritatea și valabilitatea datelor personale deținute de **Universitatea Națională de Știință și Tehnologie POLITEHNICA București** la un moment dat.

Odată identificată încălcarea de securitate a datelor cu caracter personal, se va pune în aplicare respectarea Planului de răspuns la incidentele de securitate a datelor cu caracter personal – Anexa 1.

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

5.2. Care sunt încălcările de securitate ce trebuie notificate către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)?

În momentul în care se constată sau există suspiciunea apariției unei încălcări de securitate, se impune analizarea și stabilirea probabilității și gravității riscului de afectare a drepturilor și libertăților persoanelor vizate.

În procesul de evaluare a riscului în balanță cu drepturile și libertățile persoanelor vizate, este importantă focusarea pe potențialele consecințe negative asupra individului.

În cazul în care se constată existența riscului de impactare a vieții private a persoanei vizate, atunci apare obligația notificării **ANSPDCP.** Dacă se constată că drepturile și libertățile persoanei vizate nu sunt afectate și autoritatea de supraveghere nu trebuie informată, universitatea trebuie să fie capabilă să justifice și să documenteze această decizie.
Aliniatul (85) din Regulamentul 2016/679 explică:
"Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză. Prin urmare, de îndată ce a luat cunoștință de producerea unei încălcări a securității datelor cu caracter personal, operatorul ar trebui să notifice această încălcare autorității de supraveghere, fără întârziere".

Aceasta înseamnă că anumite incidente de securitate a datelor personale pot avea efecte adverse asupra indivizilor, în timp ce altele nu impactează drepturile și libertățile persoanelor vizate, ci doar conduc la inconveniențe privind exercitarea sarcinilor de serviciu ale operatorului.

De exemplu, afectarea unei baze de date proprii sau a unor înregistrări pe calculatorul de serviciu prin alterarea accidentală a anumitor date, dar pentru care a fost constituit "back-up" al informației, nu constituie o breșă de securitate ce ar trebui raportată la autoritatea de supraveghere. În schimb, în cazul în care distrugerea sau blocarea bazei de date este o urmare a unui atac cibernetic, existând riscul de furt de informații sau de identitate, autoritatea de supraveghere va trebui notificată.

5.3. Ce rol are „persoana împuternicită" în identificarea și notificarea breșelor de securitate?

În cazul utilizării unui procesator (" persoană împuternicită") pentru a prelucra date cu caracter personal în numele universității și acesta suferă un incident de securitate a datelor personale, în conformitate cu Art. 33 (2) din Regulament, procesatorul trebuie să informeze universitatea

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

(aceasta având calitate de operator), fără întârzieri nejustificate, după ce a luat la cunoștință de acest incident.

Ca exemplificare, instituția are contract cu o firma de IT în vederea prelucrării și stocării datelor angajaților, cu scopul îndeplinirii obligațiilor legale ce îi revin în legătură cu contractul individual de muncă. Firma de IT detectează un atac cibernetic asupra rețelei sale informatice, care are ca efect acccsarca ilegală a datelor personale ale clienților săi. Având în vedere că această situație reprezintă o breșă de securitate, firma de IT are obligația de a notifica imediat instituția despre incident, iar universitatea, la rândul său, în calitate de operator, trebuie să notifice autoritatea de supraveghere.

Un astfel de mod de lucru permite universității să adopte măsuri urgente referitoare la minimizarea riscurilor privind afectarea drepturilor și libertăților persoanelor vizate, cât și în ceea ce privește obligațiile de notificare a Autorității de Supraveghere și de informare a persoanei vizate, atunci când este cazul.

În cazul utilizării unui procesator ("persoană împuternicită"), universitatea va trebui să încheie un contract cu acesta, contract ce este necesar să includă un angajament de confidențialitate și de conformare la GDPR.

5.4. Ce perioadă de timp este reglementată pentru raportarea unui incident de securitate?

În cazul în care are loc o încălcare a securității datelor cu caracter personal, universitatea, în calitatea sa de operator, notifică acest fapt Autorității de Supraveghere competente în temeiul articolului 55, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este puțin probabil să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea către autoritatea de supraveghere nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație motivată pentru întârziere.

Dacă se cunoaște faptul că a avut loc o încălcare a securității datelor cu caracter personal, întârzierea raportării incidentului reduce timpul responsabilului cu protecția datelor de a analiza și a formula un răspuns oficial către ANSPDCP în termenul legal.

5.5. Ce categorii de informații sunt necesare pentru notificarea încălcării securității datelor personale către autoritatea de supraveghere?

Când universitatea raportează o încălcare de securitate către autoritatea de supraveghere, aceasta este obligată să furnizeze următoarele informații:

- o descriere a naturii incidentului de securitate apărut;
- categoriile și numărul aproximativ de indivizi afectați sau posibil să fie afectați;
- categoriile și cantitatea aproximativă de date cu caracter personal impactate;

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

- numele și detaliile de contact ale responsabilului cu protecția datelor și ale altor persoane relevante pentru situația dată;
- o descriere a consecințelor breșei de securitate asupra drepturilor și libertăților persoanelor vizate impactate;
- o descriere a măsurilor luate sau propuse a fi implementate de către operator, în vederea minimizării sau remedierii efectelor negative asupra persoanelor vizate.

Aceste informații sunt colectate în momentul raportării interne a incidentului de securitate de către persoana care a constatat evenimentul, prin completarea "Formularului intern pentru raportarea incidentului de securitate" - Anexa 2. Informațiile colectate prin formular sunt actualizate sau completate cu date noi, pe măsură ce se realizează cercetări asupra cauzelor declanșatoare și a efectelor și riscului de impactare a persoanei vizate.

5.6. Cum se procedează în cazul în care nu sunt disponibile toate informațiile necesare notificării încălcării securității datelor

Regulamentul GDPR recunoaște că nu întotdeauna este posibil ca un incident de securitate să fie investigată în 72 de ore, pentru a înțelege exact ce s-a întâmplat și ce este de făcut pentru a limita efectele negative ale incidentului asupra persoanelor vizate.

Astfel, Art. 33(4) stipulează: "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".

Un astfel de exemplu ar fi momentul în care instituția ar constata o intruziune în rețeaua informatică și ar conștientiza că fișiere cu date personale au fost ilegal accesate, dar nu a identificat încă modul în care s-a produs atacul informatic, în ce măsură datele au fost accesate sau dacă au fost copiate în vederea utilizării frauduloase în detrimentul drepturilor și libertăților persoanelor vizate afectate.

În astfel de condiții, trebuie trimisă către autoritatea de supraveghere o primă notificare în 72 de ore de la aflarea incidentului, alături de precizarea faptului că nu sunt încă disponibile toate detaliile, dar se așteaptă ca rezultatele investigațiilor să fie gata în câteva zile. Imediat ce sunt accesibile toate informațiile referitoare la incident, acestea vor fi trimise fără întârziere către autoritatea de supraveghere, în vederea completării notificării inițiale.

5.7. Când este necesar să fie informate persoanele vizate despre incidentul de securitate apărut?

În conformitate cu Art. 34 din GDPR, în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

Un "risc ridicat" reprezintă acea situație în care nivelul de afectare a vieții private a persoanei vizate este mai mare decât pragul necesar pentru informarea Autorității de Supraveghere. Așa cum deja s-a precizat anterior, este necesar să se evalueze severitatea impactului potențial sau actual al incidentului asupra individului. Cu cât consecințele sunt mai mari, cu atât riscul este mai mare și, în astfel de situații, trebuie să fie informată prompt persoana vizată, mai ales dacă este nevoie să se limiteze de urgență daunele. Unul dintre motivele principale de informare a persoanei vizate este tocmai în scopul de a o ajuta să se protejeze și în mod direct de efectele incidentului de securitate.

Pentru exemplificare, se consideră situația în care o bază de date cu datele personale ale angajaților din universitate a fost accesată fraudulos. Având în vedere efectele potențiale ale furtului de identitate asupra
vieții private a fiecăruia și necesitatea minimizării acestora, este important ca persoana vizată să fie informată prompt.

Pe de altă parte, dacă în universitate se constată că un angajat a șters accidental niște înregistrări referitoare la date de contact pentru un număr de absolvenți din baza de date proprie, dar aceste date pot fi reconstituite ulterior dintr-un fișier de back-up, riscul de afectare a individului este redus și doar pe termen foarte scurt, ceea ce nu obligă la informarea persoanei vizate.

Este important de menționat că, dacă universitatea decide că nu e cazul să informeze persoana vizată despre incidentul de securitate apărut, în continuare rămâne obligația de a notifica autoritatea de supraveghere, această sarcină nefiind necesar a se respecta doar dacă se poate demonstra că nu există niciun risc de a fi afectate drepturile și libertățile persoanei vizate. Trebuie de asemenea precizat că autoritatea de supraveghere poate să solicite universității sa informeze persoanele vizate, în cazul în care consideră că există un nivel ridicat de risc.

Indiferent de gradul de risc al incidentului și de acțiunile adoptate în ceea ce privește notificarea Autorității de Supraveghere și a persoanei vizate, universitatea, în calitate de operator, trebuie să poată argumenta și documenta decizia aleasă, în concordanță cu prevederile GDPR.

Art. 34 din GDPR precizează:

(1) În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.
(2) În informarea transmisă persoanei vizate prevăzută la alineatul (1) din prezentul articol se include o descriere într-un limbaj clar și simplu a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin informațiile și măsurile menționate la articolul 33 alineatul (3) literele (b), (c) și (d).

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

(3) Informarea persoanei vizate menționată la alineatul (1) nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită:

a) operatorul 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) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate menționat la alineatul (1) nu mai este susceptibil să se materializeze;

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

(4) În cazul în care operatorul nu a comunicat deja încălcarea securității datelor cu caracter personal către persoana vizată, autoritatea de supraveghere, după ce a luat în considerare probabilitatea ca încălcarea securității datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condițiile menționate la alineatul (3) sunt îndeplinite.

5.8. Ce informații trebuie furnizate persoanelor vizate, când le comunicăm despre apariția incidentului de securitate

În cazul necesității notificării unei breșe de securitate a datelor cu caracter personal către indivizii afectați, universitatea trebuie să comunice, într-un limbaj simplu și clar, cel puțin următoarele informații:

- numele responsabilului cu protecția datelor sau al unui alt punct de contact unde poate obține mai multe informații;
- o descriere a posibilelor consecințe ce pot apărea ca urmare a incidentului de securitate;
- o descriere a măsurilor adoptate sau propuse a fi adoptatc în vederea limitării sau anulării efectelor incidentului de securitate.

5.9. Ce alți pași se recomandă a fi făcuți de către universitate, în conformitate cu GDPR, ca răspuns la un incident de securitate?

Universitatea trebuie să se asigure că există o evidență clară a tuturor incidentelor de securitate identificate, indiferent dacă acestea au fost sau nu raportate către autoritatea de supraveghere sau a fost sau nu necesară informarea persoanei vizate, prin completarea de către responsabilul cu protecția datelor cu caracter personal a „Registrului de evidență a încălcărilor de securitate" – Anexa 3.

În conformitate cu Art. 33(5) din GDPR, "operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație permite autorității de supraveghere să verifice conformitatea cu prezentul articol."

În același timp, în cazul fiecărui incident de securitate, trebuie să se investigheze dacă acesta a fost rezultatul unei erori umane sau este o eroare sistematică, iar în acest caz trebuie văzut cum poate fi
prevenită sau scăzută recurența acestui tip de incident. De multe ori, o nouă instruire imediată a personalului este considerată o măsură organizatorică absolut necesară în prevenirea unor astfel de evenimente. De asemenea, trebuie luate în calcul orice alte măsuri corective din punct de vedere tehnic pentru evitarea, pe cât posibil, a incidentelor de securitate pe viitor.

5.10. Ce se întâmplă dacă se omite notificarea autorității de supraveghere?

În contextul GDPR, autoritatea de supraveghere are următoarele competențe corective:

- de a emite avertizări în atenția operatorului sau a persoanei împuternicite de operator cu privire la posibilitatea ca operațiunile de prelucrare prevăzute să încalce dispozițiile regulamentului;
- de a emite avertismente adresate unui operator sau unei persoane împuternicite de operator în cazul în care operațiunile de prelucrare au încălcat dispozițiile prezentului regulament;
- de a da dispoziții operatorului sau persoanei împuternicite de operator să respecte cererile persoanei vizate de a-și exercita drepturile în temeiul prezentului regulament;
- de a da dispoziții operatorului sau persoanei împuternicite de operator să asigure conformitatea operațiunilor de prelucrare cu dispozițiile prezentului regulament;
- de a obliga operatorul să informeze persoana vizată cu privire la o încălcare a protecției datelor cu caracter personal;
- de a impune amenzi administrative în conformitate cu articolul 83, în completarea sau în locul măsurilor menționate la prezentul alineat, în funcție de circumstanțele fiecărui caz în parte;

În cazul în care se omite (voit sau accidental) să se notifice autoritatea de supraveghere, atunci când acest fapt este necesar, se pot impune amenzi administrative până la 10.000.000 de euro sau, în cazul unei întreprinderi, de până la 2% din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare.

Atunci când se ia decizia dacă să se impună o amendă administrativă și decizia cu privire la valoarea amenzii administrative în fiecare caz în parte, se acordă atenția cuvenită următoarelor aspecte:

- natura, gravitatea și durata încălcării, ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și de numărul persoanelor vizate afectate și de nivelul prejudiciilor suferite de acestea;

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

- dacă încălcarea a fost comisă intenționat sau din neglijență;
- orice acțiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de persoana vizată;
- gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ţinându-se seama de măsurile tehnice și organizatorice implementate de aceștia în temeiul articolelor 25 și 32;
- eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;
- gradul de cooperare cu autoritatea de supraveghere pentru a remedia încălcarea și a atenua posibilele efecte negative ale încălcării;
- categoriile de date cu caracter personal afectate de încălcare;
- modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere, în special dacă și în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;

În concluzie, este foarte important să fie pus în practică un proces bine structurat de raportare a incidentelor de securitate, care să asigure identificarea și notificarea la timp a acestui tip de incident, în scopul conformării la prevederile GDPR și a evitării sancțiunilor sau amenzilor din parte autorității de supraveghere.

Rector,
Mihnea Cosmin COSTOIU

[redacted]

Întocmit,
Șef serviciu,
Serviciul GDPR și Documente Secrete
Ioana MOCANU-PARASCHIV

[redacted]

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

Anexa 1

Plan de răspuns la incidentele de securitate a datelor cu caracter personal

1. **Primul pas este stoparea producerii efectelor incidentului.** Acțiunile specifice ce vor trebui aplicate vor fi evaluate în funcție de circumstanțele incidentului. În continuare trebuie respectate următoarele puncte:

a) **Datele nu trebuie modificate**. - Dacă are loc orice fel de modificare a datelor din sistem, poate fi afectată desfășurarea în condiții normale a potențialului litigiu.

b) **Datele trebuie accesate în original doar în circumstanțe excepționale.** Un specialist va folosi instrumentele necesare pentru a copia orice fel de date existente în memorie. Toate analizele vor avea loc asupra copiilor, iar datele originale nu trebuie accesate decât în cazuri excepționale.

c) **Se va păstra întotdeauna o dovadă a ceea ce s-a făcut**. Unde este posibil și relevant, primele persoane venite la locul incidentului, se încurajează să fotografieze și să înregistreze video, atâta timp cât nimic nu este atins.

d) Trebuie colectate informațiile de bază, iar acestea pot include:
   - Fotografii sau înregistrări video ale mesajelor/informațiilor relevante;
   - Înregistrarea manuală a cronologiei incidentului;
   - Documentele originale, inclusiv înregistrări despre persoanele care le-au găsit, unde și când;
   - Detalii despre orice fel de martor (în cazul în care putem vorbi de o încălcare fizică).

Unde este posibil, odată colectate, dovezile trebuie păstrate într-un loc sigur unde nu pot fi modificate și protejate prin aplicarea unui sigiliu. Dovezile pot fi necesare pentru o analiză ulterioară a cauzei incidentului și/sau ca probă informatică în dosarele judecătorești civile sau penale. Ulterior, trebuie stabilită o imagine clară asupra incidentului. Întinderea acestuia și impactul implicațiilor trebuie analizate anterior oricăror acțiuni privind izolarea. Înregistrările pot fi examinate pentru a reconstitui secvențe ale evenimentelor, trebuie folosite doar copii ale înregistrărilor care nu au fost modificate.

2. Concomitent cu punctul 1, **structurile care prelucrează datele** cu caracter personal **au obligația să înștiințeze, fără întârzieri nejustificate, responsabilul cu protecția datelor** despre încălcarea produsă (pentru POLITEHNICA București – datele de contact ale responsabilului sunt: e-mail - dpo@upb.ro, tel: 021 402 9012; pentru Centrul Universitar Pitești - datele de contact ale responsabilului sunt: dpo-pitești@upb.ro, tel: 0348 453 121). Persoana care a constatat evenimentul va completa "Formularul intern pentru raportarea incidentului de securitate" - Anexa 1 și i-o va transmite responsabilului cu protecția datelor cât mai repede posibil.
3. Responsabilul cu protecția datelor informează de îndată conducerea instituției;
4. Structura în care a avut loc incidentul, ia măsurile necesare privind acțiunile de reparare a prejudiciilor cauzate de incident. Aceste acțiuni ar trebui să aibă drept obiectiv

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

rezolvarea problemei curente și să prevină un nou astfel de incident. **Orice vulnerabilități care au dus la incident trebuie identificate.**

5. Structurile care prelucrează datele cu caracter personal, informează persoana/persoanele vizate în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice (cu excepția cazului în care s-au aplicat măsuri de protecție tehnice și organizatorice eficace sau alte măsuri care asigură faptul că riscul nu mai este susceptibil să se materializeze).
6. Responsabilul cu protecția datelor conlucrează cu structura care a sesizat încălcarea securității datelor cu caracter personal în vederea analizării acestei încălcări;
7. Responsabilul cu protecția datelor notifică ANSPDCP cu privire la încălcarea securității datelor cu caracter personal.
8. În timpul etapei de recuperare, sistemele ar trebui aduse la starea inițială de către structura responsabilă, la condiția de dinainte de incident, iar ulterior să fie implementate acțiunile necesare pentru a stopa orice vulnerabilitate care a dus la crearea incidentului.
9. Responsabilul cu protecția datelor monitorizează starea incidentului și se asigură ca au fost implementate măsurile corective și preventive.
10. Responsabilul cu protecția datelor înregistrează evenimentul în „Registrului de evidență a încălcărilor de securitate" – Anexa 3.

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

Anexa 2

FORMULAR INTERN PENTRU RAPORTARE BREȘĂ DE SECURITATE

1. INFORMAȚII DE CONTACT		
1.1.	Raportat de:	
1.2.	Departament/Facultate/Serviciu:	
1.3.	Funcția:	
1.4.	Adresa de email:	
1.5.	Nr. telefon:	
1.6.	Data:	

2. LISTA DE DISTRIBUȚIE		
2.1.	Responsabil cu protecția datelor (DPO): *obligatoriu	
2.2.	Șef Direcție/Serviciu, Decan Facultate, Prorector coordonator al structurii, alt coordonator de structură, după caz: *obligatoriu	
2.3.	Dir. Informatizare (dacă este cazul):	
2.4.	Alte pers. relevante pt. soluționare incident:	

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

3. INFORMAȚII DESPRE INCIDENT		
3.1.	Data și ora de început a incidentului:	
3.2.	Data și ora identificării incidentului:	
3.3.	Numele utilizatorului/utilizatorilor datelor personale impactate:	
3.4.	Caracterul incidentului (confidențialitate, integritate, disponibilitate):	
3.5.	Natura și conținutul datelor personale afectate sau la risc. Datele impactate erau criptate?	
3.6.	Tip suport date personale afectate (pe suport de hârtie, electronic în calculatorul personal, site web, email, echipamente electronice mobile de back-up, etc):	
3.7.	Număr înregistrări de date personale afectate:	
3.8.	Număr de persoane vizate:	
3.9.	Categorii de persoane vizate:	
3.10.	Posibile cauze identificate:	

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

4. DESCRIERE INCIDENT		
4.1.	Rezumatul incidentului (incluzând detalii ref. locație, contextul în care a fost identificat, efecte constatate, riscuri de afectare, posibilitate de minimizare efecte, cauză accidentală sau intenționată):	
4.2.	Este implicată o altă firmă (procesator/partener) în prelucrarea datelor personale impactate?	☐ DA Precizați numele procesatorului/partenerului, numele reprezentantului acestuia, date de contact, în măsura în care sunt cunoscute ☐ NU
4.3.	Măsuri de securitate imediată puse în practică de către pers./dept. care a identificat incidentul :	
4.4.	Progresul realizat în procesul de minimizare a riscurilor:	

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

5. INFORMATII ACTUALIZATE REF. INCIDENT **Se completează de către Responsabilul GDPR, în colaborare cu factorii de decizie din **Universitatea Națională de Știință și Tehnologie POLITEHNICA București***		
5.1.	Analiza nivelului de risc de afectare a drepturilor și libertăților persoanei vizate:	
5.2.	Măsuri organizatorice și tehnice implementate sau propuse a fi implementate în vederea minimizării riscului de afectare a persoanei vizate:	
5.3.	Documentarea necesității dc a notifica sau nu Autoritatea de supraveghere:	
	Data notificării (dacă este cazul):	
5.4.	Documentarea necesității de a informa sau nu persoana vizată:	
	Data informării (dacă este cazul):	

Dată raportare incident:
.....
Semnătură persoană care raportează incidentul:
.....

Dată închidere formular:
.....
Nume/Semnătură
.....

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro

Anexa 3

Registru de evidență a încălcărilor de securitate

-anul-

Nr. crt.	Numele și datele de contact ale operatorului, reprezentantului operatorului și ale DPO	Facultate/ Departament/ Direcție/ Serviciu/ Birou	Tipul incidentului și modul în care a avut loc acesta	Caracterul încălcării securității datelor	Natura și conținutul datelor afectate de incident	Data și ora survenirii incidentului	Data și ora descoperirii incidentului	Persoana care a descoperit incidentul	Persoana responsabilă de domeniul în care a survenit incidentul	Gradul de probabilitate privind afectarea drepturilor persoanelor vizate	Măsurile luate anterior pentru prevenirea unui astfel de incident	Măsuri luate pentru a opri incidentul/ ameliora situația	Notificare ANSPDCP/ Notificare persoane vizate	Numărul aproximativ și categoriile persoanelor vizate afectate	Consecințele probabile ale incidentului
1.															
2.															
3.															

***Notă**

Coloana *tipul incidentului și modul în care a avut loc acesta* se va completa cu termeni precum: distrugere, pierdere, modificare, divulgare neautorizată, acces neautorizat etc; prin e-mail, în mod fizic etc.

Coloana *caracterul încălcării securității datelor* se va completa cu termeni precum: confidențialitate, integritate, disponibilitate.

Coloana *persoana care a descoperit incidentul* și *persoana responsabilă de domeniul în care a survenit incidentul* se va completa prin indicarea numelui, prenumelui și funcției persoanei.

Coloana *gradul de probabilitate privind afectarea drepturilor persoanelor vizate* se va completa prin indicarea unuia dintre următoarele grade: inexistent, infim, mic, mediu, ridicat, absolut.

Coloana *necesitatea de a comunica incidentul Autorității Naționale/Persoanelor vizate* se va completa prin indicarea răspunsurilor după modelul: DA/NU, DA/DA, NU/NU.

Coloana *numărul aproximativ și categoriile persoanelor vizate afectate* se va completa în ceea ce privește categoria persoanelor vizate prin folosirea noțiunilor precum: minori, angajați, cetățeni, pacienți, clienți, copii etc.

Inginerie și cercetare pentru viitor
Splaiul Independenței 313, sector 6, Mun. București, RO 060042, România
E-mail: dpo@upb.ro
www.upb.ro