POLITICA

PRIVIND RECUNOAŞTEREA ÎNCĂLCĂRILOR SECURITĂȚII

DATELOR CU CARACTER PERSONAL

ŞI

MODUL DE ACŢIONARE ÎN CAZUL NEDORIT AL APARIŢIEI ACESTORA

1. SCOP GENERAL

Scopul acestei politici este de a informa şi sensibiliza toate structurile operatorului referitor la identificarea utilizării frauduloase, neautorizate a datelor cu caracter personal deţinute de operator, cât şi a modului de a acţiona şi raporta în cazul apariţiei nedorite a unor astfel de incidente.

2. OBIECTIVE

Această politică are ca obiective principale:

- Să constituie un instrument în sprijinul fiecărui membru al personalului operatorului, în vederea recunoaşterii unei eventuale încălcări a securității;
- Să ajute la evitarea şi prevenirea utilizării frauduloase, neautorizate, ilegale, a pierderii sau distrugerii accidentale a datelor cu caracter personal deţinute în operator;
- Să contribuie la stabilirea unui mod de lucru transparent privind raportarea internă de către angajaţi a unor astfel de incidente, atât pe linie ierarhică, cât şi către responsabilul cu protecţia datelor din operator;
- Să ajute la evaluarea riscului unui incident de securitate cu privire la gradul de afectare a drepturilor şi libertăţilor persoanelor vizate;
- Să ghideze factorii de decizie din cadrul operatorului privind modul de administrare a unor astfel de incidente de securitate, incluzând condiţiile de raportare către Autoritatea naţională de supraveghere a prelucrării datelor cu caracter personal şi informarea persoanei vizate.

3. DEFINIŢII

În Regulamentul GDPR sunt prevăzute următoarele definiţii, 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;

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

4. NOŢIUNI PRIVIND ÎNCĂLCĂRILE DE SECURITATE A DATELOR CU CARACTER PERSONAL, ÎN CONTEXTUL GDPR

4.1. Ce este o încălcare a securității datelor cu caracter personal?

O încălcare de securitate a datelor cu caracter personal presupune o breșă de securitate care conduce, în mod accidental sau intenţionat, la distrugerea, pierderea, alterarea datelor cu caracter personal sau divulgarea, permiterea accesului neautorizat la acestea.

Următoarele acţiuni ar putea conduce către apariţia unor încălcări a securității:

- Accesul neautorizat al unei terţe părţi la baze de date personale ale operatorului;
- Permiterea accesului unei persoane neautorizate la un echipament de calcul sau intr-un spaţiu unde sunt stocate date cu caracter personal;
- Divulgarea accidentală sau intenţionată a unor date personale colectate/prelucrate/stocate de către operator;
- Trimiterea de informaţii/fişiere, ce conţin date personale, către un destinatar greşit;
- 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 deţinute de operator;
- Pierderea sau distrugerea accidentală a bazelor de date personale, fără posibilitatea reconstituirii acestora într-un termen rezonabil, în vederea respectării “dreptului de acces” al persoanei vizate;
- Pierderea posibilităţii de accesare a datelor cu caracter personal în urma criptării frauduloase a bazelor de date, ca efect al unui atac cibernetic asupra reţelei informatice a operatorului.

Pe scurt, breşa de securitate a datelor cu caracter personal reprezintă orice incident de securitate care afectează confidenţialitatea, integritatea şi disponibilitatea datelor cu caracter personal deţinute de operator la un moment dat.

4.2. Care sunt breşele de securitate ce trebuie notificate către Autoritatea Naţională de Supraveghere?

În momentul în care se constată sau există suspiciunea apariţiei unei încălcări a securităţii, se impune analizarea şi stabilirea probabilităţii şi gravităţii riscului de afectare a drepturilor şi libertăţilor persoanelor vizate.

În procesul de evaluare a riscului în balanţă cu drepturile şi libertăţile persoanelor vizate, este importantă focusarea pe potenţialele consecinţe negative asupra individului.

În cazul în care se constată existenţa riscului de impactare a vieţii private a persoanei vizate, atunci apare obligaţia notificării **Autorităţii Naţionale de Supraveghere**. Dacă se constată că drepturile şi libertăţile persoanei vizate nu sunt afectate şi Autoritatea de Supraveghere nu trebuie informată, operatorul trebuie să fie capabil să justifice şi să documenteze această decizie.

Aliniatul (85) din Regulamentul 2016/679 explică:

“Dacă nu este soluţionată la timp şi într-un mod adecvat, o încălcare a securităţii 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 reputaţiei, pierderea confidenţialităţii 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 cunoştinţă de producerea unei încălcări a securităţii datelor cu caracter personal, operatorul ar trebui să notifice această încălcare autorităţii de supraveghere, fără întârziere”.

Aceasta înseamnă că anumite incidente de securitate a datelor cu caracter personal pot avea efecte adverse asupra indivizilor, în timp ce altele nu impactează drepturile şi libertăţile persoanelor vizate, ci doar conduc la inconvenienţe privind exercitarea sarcinilor de serviciu ale prelucrătorului.

De exemplu, afectarea unei baze de date proprii sau a unor înregistări pe calculatorul de serviciu prin alterarea accidentală a anumitor date, dar pentru care a fost constituit “back-up” al informaţiei, nu constituie o breşă 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 informaţii sau de identitate, Autoritatea de Supraveghere va trebui notificată.

Notificarea încălcării securității către Autoritatea de Supraveghere se va face prin intermediul formularelor online disponibile de pe site-ul web al acesteia

www.dataprotection.ro/formulare/formularbresagdpr

Pentru a stabili și identifica mai ușor pașii privind notificarea încălcărilor de securitate a datelor cu caracter personal se aplică **Anexa nr. 2 Diagrama cerințelor de notificare**.

4.3. Ce rol are „persoana împuternicită” în identificarea şi notificarea încălcărilor securității?

În cazul utilizării unui procesator (”persoană împuternicită”) pentru a prelucra date cu caracter personal în numele operatorului şi acesta suferă o breşă de securitate a datelor cu caracter personal, în

conformitate cu Art. 33 (2) din Regulament, procesatorul trebuie să informeze operatorul, fără întârzieri nejustificate, după ce a luat la cunoştinţă de acest incident.

Ca exemplificare, instituţia are contract cu o firma de IT în vederea prelucrării şi stocării datelor angajaţilor, cu scopul îndeplinirii obligaţiilor legale ce îi revin în legătură cu contractul individual de muncă. Firma de IT detectează un atac cibernetic asupra reţelei sale informatice, care are ca efect accesarea ilegală a datelor cu caracter personal ale clienţilor săi. Având în vedere că această situaţie reprezintă o breşă de securitate, firma de IT are obligaţia de a notifica imediat instituţia despre incident, iar operatorul, la rândul său, în calitate de operator, trebuie să notifice Autoritatea de Supraveghere.

Un astfel de mod de lucru permite operatorului să adopte măsuri urgente referitoare la minimizarea riscurilor privind afectarea drepturilor şi libertăţilor persoanelor vizate, cât şi în ceea ce priveşte obligaţiile de notificare a Autorităţii de Supraveghere şi de informare a persoanei vizate, atunci când este cazul.

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

4.4. Ce perioadă de timp este reglementată pentru raportarea unei încălcălcări a securității?

În cazul în care are loc o încălcare a securităţii datelor cu caracter personal, instituția, în calitatea sa de operator, notifică acest fapt Autorităţii de Supraveghere competente în temeiul articolului 55, fără întârzieri nejustificate şi, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoştinţă de aceasta, cu excepţia cazului în care este puţin probabil să genereze un risc pentru drepturile şi libertăţile persoanelor fizice.

În cazul în care notificarea către Autoritatea de Supraveghere nu are loc în termen de 72 de ore, aceasta este însoţită de o explicaţie motivată pentru întârziere.

4.5. Ce categorii de informaţii sunt necesare pentru notificarea breşei de securitate către Autoritatea de Supraveghere?

Când operatorul raportează o breşă de securitate către Autoritatea de Supraveghere, acesta este obligat să furnizeze următoarele informaţii:

- o descriere a naturii incidentului de securitate apărut;
- categoriile şi numărul aproximativ de indivizi afectaţi sau posibil să fie afectaţi;
- categoriile şi cantitatea aproximativă de date cu caracter personal impactate;
- numele şi detaliile de contact ale responsabilului cu protecţia datelor şi ale altor persoane relevante pentru situaţia dată;
- o descriere a consecinţelor breşei de securitate asupra drepturilor şi libertăţilor persoanelor vizate impactate;
- o descriere a măsurilor luate sau propuse a fi implementate de către operator, în vederea minimizării sau remedierii efectelor negative ale breşei de securitate asupra persoanelor vizate.

4.6. Cum se procedează în cazul în care nu sunt disponibile toate informaţiile necesare notificării breşei de securitate.

Regulamentul GDPR recunoaşte că nu întotdeauna este posibil ca o breşă de securitate să fie investigată în 72 de ore, pentru a înţelege exact ce s-a întâmplat şi ce este de făcut pentru a limita efectele negative ale incidentului asupra persoanelor vizate.

Astfel, Art. 33(4) stipulează: "Atunci când şi în măsura în care nu este posibil să se furnizeze informaţiile în acelaşi timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate".

Un astfel de exemplu ar fi momentul în care instituţia ar constata o intruziune în reţeaua informatică şi ar conştientiza că fişiere 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 şi libertăţilor persoanelor vizate afectate.

În astfel de condiţii, 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 aşteaptă ca rezultatele investigaţiilor să fie gata în câteva zile. Imediat ce sunt accesibile toate informaţiile referitoare la incident, acestea vor fi trimise fără întârziere către Autoritatea de Supraveghere, în vederea completării notificării iniţiale.

4.7. 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 securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

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

Pentru exemplificare, se consideră situaţia în care o bază de date cu datele personale ale angajaţilor din operator a fost accesată fraudulos. Avand în vedere efectele potenţiale ale furtului de identitate asupra vieţii private a fiecăruia şi necesitatea minimizării acestora, este important ca persoana vizată să fie informată prompt.

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

Este important de menţionat că dacă operatorul decide că nu e cazul să informeze persoana vizată despre incidentul de securitate apărut, în continuare rămâne obligaţia 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 şi libertăţile persoanei vizate. Trebuie de asemenea precizat că Autoritatea de Supraveghere poate să solicite operatorului sa informeze persoanele vizate, în cazul în care consideră că există un nivel ridicat de risc.

Indiferent de gradul de risc al incidentului şi de acţiunile adoptate în ceea ce priveşte notificarea Autorităţii de Supraveghere şi a persoanei vizate, operatorul, în calitate de operator, trebuie să poată argumenta şi documenta decizia aleasă, în concordanţă cu prevederile GDPR.

Art. 34 din GDPR precizează:

(1) În cazul în care încălcarea securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile 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 şi simplu a caracterului încălcării securităţii datelor cu caracter personal, precum şi cel puţin informaţiile şi măsurile menţionate la articolul 33 alineatul (3) literele (b), (c) şi (d).

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

a) operatorul a implementat măsuri de protecţie tehnice şi organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securităţii 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 şi libertăţile persoanelor vizate menţionat la alineatul (1) nu mai este susceptibil să se materializeze;

c) ar necesita un efort disproporţionat. În această situaţie, 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 securităţii datelor cu caracter personal către persoana vizată, Autoritatea de Supraveghere, după ce a luat în considerare probabilitatea ca încălcarea securităţii datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condiţiile menţionate la alineatul (3) sunt îndeplinite.

4.8. Ce informaţii trebuie furnizate persoanelor vizate, când le comunicăm despre apariţia incidentului de securitate

În cazul necesităţii notificării unei încălcare a securității a datelor cu caracter personal către indivizii afectaţi, operatorul trebuie să comunice, într-un limbaj simplu şi clar, cel puţin următoarele informaţii:

- numele responsabilului cu protecţia datelor sau al unui alt punct de contact unde poate obţine mai multe informaţii;
- o descriere a posibilelor consecinţe ce pot apărea ca urmare a incidentului de securitate;

- o descriere a măsurilor adoptate sau propuse a fi adoptate în vederea limitării sau anulării efectelor breşei de securitate.

În cazul în care încălcarea securității asupra datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertatile persoanelor fizice, SJU Bacău va informa persoanele vizate în cel mai scurt timp, fără alte întârzieri, prin documentul **"Formular de notificare a încălcării securității datelor către persoanele vizate" – Anexa nr 3**.

4.9. Ce alţi paşi se recomandă a fi făcuţi de către OPERATOR, în conformitate cu GDPR, ca răspuns la un incident de securitate?

Operatorul trebuie să se asigure că există o evidenţă clară a tuturor încălcărilor securității identificate, indiferent dacă acestea au fost sau nu raportate către Autoritatea de Supraveghere sau a fost sau nu necesară informarea persoanei vizate.

În conformitate cu Art. 33(5) din GDPR, "operatorul păstrează documente referitoare la toate cazurile de încălcare a securităţii datelor cu caracter personal, care cuprind o descriere a situaţiei de fapt în care a avut loc încălcarea securităţii datelor cu caracter personal, a efectelor acesteia şi a măsurilor de remediere întreprinse. Această documentaţie permite autorităţii de supraveghere să verifice conformitatea cu prezentul articol."

Orice încălcare a securității (indiferent de riscul generat asupra persoanelor vizate) trebuie înregistrată de DPO în documentul **"Registru incidente de securitate" - Anexa nr. 4**, care se păstrează de către Responsabilul cu protecția datelor (DPO) și de către Operator.

În acelaşi 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 recurenţa 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 încălcărilor securității pe viitor.

4.10. Ce se întamplă dacă se omite notificarea Autorităţii de Supraveghere?

În contextul GDPR, Autoritatea de Supraveghere are următoarele competenţe corective:

- de a emite avertizări în atenţia operatorului sau a persoanei împuternicite de operator cu privire la posibilitatea ca operaţiunile de prelucrare prevăzute să încalce dispoziţiile regulamentului;
- de a emite avertismente adresate unui operator sau unei persoane împuternicite de operator în cazul în care operaţiunile de prelucrare au încălcat dispoziţiile prezentului regulament;
- de a da dispoziţii operatorului sau persoanei împuternicite de operator să respecte cererile persoanei vizate de a-şi exercita drepturile în temeiul prezentului regulament;
- de a da dispoziţii operatorului sau persoanei împuternicite de operator să asigure conformitatea operaţiunilor de prelucrare cu dispoziţiile prezentului regulament;
- de a obliga operatorul să informeze persoana vizată cu privire la o încălcare a protecţiei datelor cu caracter personal;

- de a impune amenzi administrative în conformitate cu articolul 83, în completarea sau în locul măsurilor menţionate la prezentul alineat, în funcţie de circumstanţele 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 exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare.

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

- natura, gravitatea şi durata încălcării, ţinându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum şi de numărul persoanelor vizate afectate şi de nivelul prejudiciilor suferite de acestea;
- dacă încălcarea a fost comisă intenţionat sau din neglijenţă;
- orice acţiuni 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 şi organizatorice implementate de aceştia în temeiul articolelor 25 şi 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 şi a atenua posibilele efecte negative ale încălcării;
- categoriile de date cu caracter personal afectate de încălcare;
- modul în care încălcarea a fost adusă la cunoştinţa autorităţii de supraveghere, în special dacă şi 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 încălcărilor securității, care să asigure identificarea şi notificarea la timp a acestui tip de incident, în scopul conformării la prevederile GDPR şi a evitării sancţiunilor sau amenzilor din parte Autorităţii de supraveghere.

Prezentul document intră învigoare la data aprobării, iar prevederile sale sunt obligatorii pentru întregul personal al spitalului.

MANAGER,

Ec. Ion-Marius SAVIN