PROCEDURA DE NOTIFICARE A ÎNCĂLCĂRII SECURITĂȚII DATELOR PERSONALE

1. Introducere

Această procedură trebuie să fie folosită atunci când un incident de orice natură a avut loc și a avut drept rezultat sau e posibil să fi avut drept rezultat o pierdere a datelor personale pentru care organizația este operator.

Este o cerință a **Regulamentului GDPR** ca incidentele care afectează datele personale și sunt susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice să fie raportate către autoritatea de supraveghere fără întârziere și, acolo unde este posibil, în termen de cel mult 72 ore de la momentul luării la cunoștință. În cazul în care termenul de 72 ore nu este îndeplinit, trebuie furnizate motivele pentru această întârziere.

Atunci când un incident afectează datele personale, o decizie trebuie să fie luată cu privire la impactul, momentul și conținutul comunicării cu persoanele vizate. Regulamentul GDPR cere ca comunicarea să aibă loc ”fără întârziere” dacă încălcarea este susceptibilă ”să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice”.

Acțiunile descrise în acest document ar trebui să fie folosite drept îndrumări atunci când răspundem unui incident. Natura exactă a incidentului și impactul acestuia nu pot fi prevăzute cu vreun grad de certitudine și de aceea este important să se facă apel la bunul simț când decidem ce să facem. Cu toate acestea, pașii descriși aici se vor dovedi folositori pentru a ne asigura că obligațiile noastre în contextual Regulamentului GDPR sunt îndeplinite.

2. Procedura privind Notificarea Încălcării Datelor Personale

Odată ce s-a decis că a avut loc o încălcare a datelor cu caracter personal, există două părți care putea fi necesar să fie informate, conform Regulamentului GDPR. Acestea sunt:

1. Autoritatea de supraveghere
2. Persoanele vizate afectate

Nu este o concluzie de sine stătătoare că încălcare trebuie notificată; asta depinde de o analiză a riscului că încălcarea reprezintă ”***risc ridicat*** *pentru drepturile și libertățile persoanelor fizice„* (**articolul 33 din Regulamentul GDPR**). Următoarele secțiuni descriu cum trebuie luată această decizie și ce trebuie făcut dacă notificarea este necesară.

2.1. Autoritatea de Supraveghere

Autoritatea de supraveghere pentru scopurile GDPR pentru **FEDERATIA ROMANA DE GIMNASTICA** este:

Nume:	**Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal**
Adresă:	**B-dul G-ral. Gheorghe Magheru 28-30, Sector 1, cod postal 010336 Bucuresti, Romania**
Telefon:	**+40.318.059.211**

Fax:	**+40.318.059.602**
Email:	**anspdcp@dataprotection.ro**

Tabel 1 - Datele de contact ale autorității de supraveghere

2.1.1. Când decidem dacă să notificăm autoritatea de supraveghere

Regulamentul GDPR menționează că încălcarea datelor personale va fi notificată către autoritatea de supraveghere "*cu excepția cazului în care NU este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice*" (articolul 33 din Regulamentul GDPR). Acest lucru obligă organizația să analizeze nivelul de risc anterior să decidă dacă sau nu notifică autoritatea.

- Dacă datele personale au fost criptate;
- Dacă au fost criptate, puterea criptării;
- Cât de mult au fost datele pseudonimizate (*ie*. dacă persoanele fizice pot fi identificate în mod rezonabil din datele existente);
- Datele personale incluse, *ie*. nume, adresă, date personale, date biometrice;
- Volumul datelor implicate;
- Numărul persoanelor vizate afectate;
- Natura încălcării, *ie*. furt, accident etc.
- Orice alți factori ar putea fi relevanți

Părțile implicate în această procedură de risc pot include reprezentanți din următoarele arii, în funcție de natura și circumstanțele încălcării datelor personale:

- Tehnologie
- Securitatea informației
- Juridic

Metoda de analiză, deciziile care stau la baza ei, precum și concluziile trebuie să fie documentate și (contra)semnate de managementul executiv. Rezultatul acestei analize de risc ar trebui să include una din următoarele concluzii:

1. Încălcarea nu necesită notificare;
2. Încălcarea trebuie notificată doar către autoritatea de supraveghere;
3. Încălcarea trebuie notificată atât către autoritatea de supraveghere, cât și față de persoanele vizate afectate;

Aceste concluzii se pot schimba pe baza feedback-ului primit de la autoritatea de supraveghere sau alte informații care sunt descoperite ca parte a investigației privind încălcarea datelor personale.

2.1.2. Cum notificăm autoritatea de supraveghere

În cazul în care se ia decizia de a notifica autoritatea de supraveghere, Regulamentul GDPR cere ca aceasta să fie făcută "fără întârziere nejustificată și, dacă este posibil, în cel mult 72 de ore după ce a luat la cunoștință de existența acesteia" (articolul 33 din Regulamentul GDPR). Dacă există motive legitime pentru nenotificare în timp cerut, trebuie oferite justificări ca parte a notificării.

Notificarea ar trebui furnizată prin mijloace adecvate de securitate către persoanele din Tabelul 1, folosind *Formarul privind Notificarea Încălcării Securității Datelor Personale* drept template.

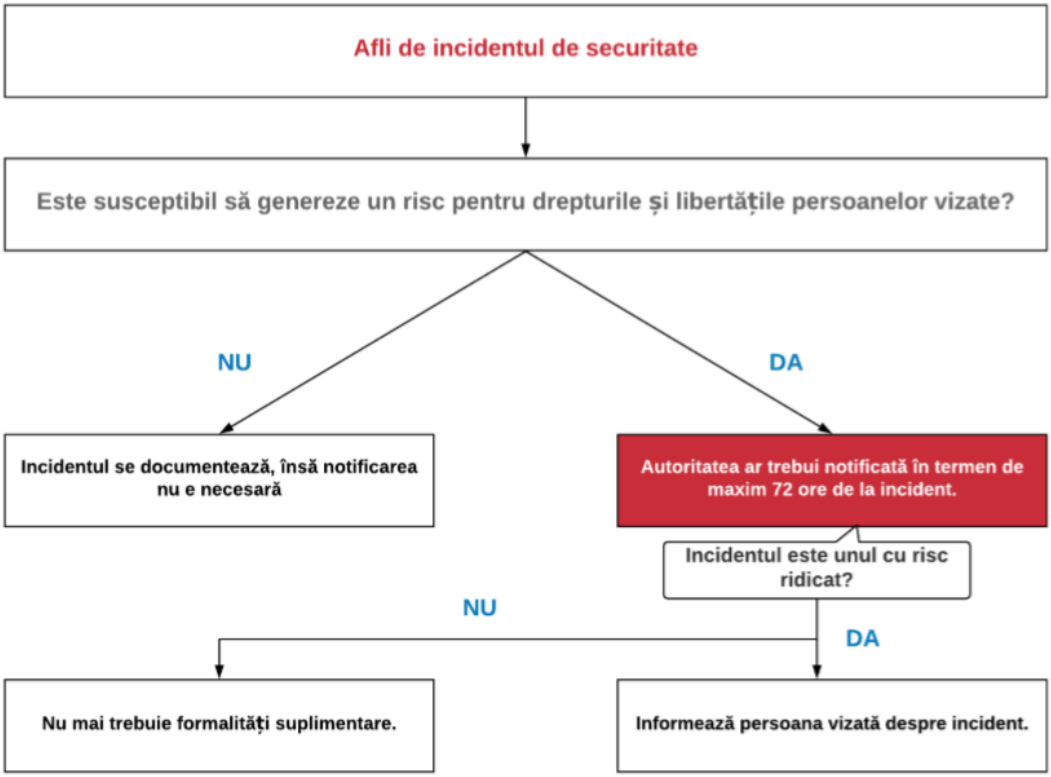
Următoarele informații ar trebuie incluse în notificare:

a) Natura încălcării securității datelor personale incluzând, acolo unde este posibil:
   i. Categoriile și numărul aproximativ de persoane vizate implicate;
   ii. Categoriile și numărul aproximativ de înregistrări ale datelor personale implicate;
b) O descriere a consecințelor posibile ale încălcării securității datelor personale;
c) O descriere a măsurilor luate sau propuse pentru a fi luate în legătură cu încălcarea securității datelor personale, incluzând, acolo unde este fezabil, măsurile luate pentru diminuarea efectelor;
d) Dacă notificarea depășește termenul de 72 ore, motivul pentru care nu a fost notificată anterior.

Este recomandat să obțineți o notificare scrisă de la autoritatea de supraveghere că notificarea a fost primită, inclusiv cu data și ora la care a fost primită. Acolo unde este necesar, Regulamentul GDPR permite ca informațiile să fie furnizate în etape, dar fără întârziere.

Documentația în cazul încălcării datelor cu caracter personal, inclusive efectele și remedii luate, vor face parte din *Procedura de Răspuns la Incidentul de Securitate.*

2.2. Persoanele Vizate



2.2.1. Notificăm sau nu persoanele vizate

Regulamentul GDPR prevede că o încălcare a securității datelor personale va fi notificată către persoanele vizate atunci când *”este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice*” (articolul 34). A se vedea adăugarea cuvântului ”ridicat” pe lângă definiția dată de articolul 33.

Analiza de risc efectuată mai devreme în această procedură (secțiunea 2.1.1) va determina dacă riscul vis-à-vis de drepturile și libertățile persoanelor vizate afectat este suficient de ridicat încât să justifice notificarea acestora.

Cu toate acestea, dacă ulterior au fost luate măsuri pentru a diminua riscul ridicat față de persoanele vizate, ca incidental să nu se mai repete, notificarea către persoanele vizate nu mai este cerută de Regulamentul GDPR.

De asemenea, notificarea către persoanele vizate nu mai este cerută de GDPR atunci când ”*ar implica un efort disproporționat”* (articolul 34). Totuși, o procedură de comunicare publică ar trebui folosită în cazul asta.

Țineți minte că această procedură se poate schimba ca urmare a feedback-ului primit din partea autorității de supraveghere și pe măsură ce sunt descoperite alte informații ca parte a investigației asupra incidentului.

2.2.2. Cum să notificăm persoanele vizate

Odată ce s-a decis că încălcarea justifică notificarea persoanelor vizate afectate, Regulamentul GDPR cere ca aceasta să fie făcută fără întârziere.

Notificarea ”*va descrie într-un limbaj clar și simplu a caracterului încălcării securității datelor cu caracter personal*” (articolul 34) și trebuie de asemenea să includă:

a) numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
b) o descriere a consecințelor probabile ale încălcării securității datelor cu caracter personal;
c) o descriere a măsurilor luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

Pe lângă condițiile cerute de Regulamentul GDPR, ar putea fi necesar să oferiți sfaturi persoanelor vizate vis-à-vis de acțiunile pe care acestea le pot lua pentru a reduce riscul asociat cu încălcarea securității datelor personale.

În majoritatea cazurilor, cel mai bine va fi să notificați persoanele vizate afectate prin e-mail, scrisoare sau ambele pentru a vă asigura că mesajul a fost recepționat și că au o posibilitatea de a lua orice acțiune necesară.

Politică aprobată în data de:	**15/03/2022**
Politica devine operațională din data de:	**15/03/2022**