

Procedură de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

CONTINUTUL PROCEDURII

SCOP: Această procedură stabilește:

1. Un set unitar de reguli care reglementează activitatea de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, conform legislației europene prin aplicarea Regulamentului nr. 679/2016;

2. Responsabilitățile privind activitatea de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal în cadrul **ALCOS BIOPROD SRL**, precum și cele privind întocmirea, avizarea și aprobarea documentelor aferente acestor activități.

Procedura de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal prezintă măsurile luate de **ALCOS BIOPROD SRL** pentru a proteja drepturile pe care le au persoanele fizice vizate de prelucrarea datelor cu caracter personal, conform legislației europene prin aplicarea Regulamentului nr. 679/2016 și interesele legitime ale acestor persoane ale caror date au ajuns în posesia firmei **ALCOS BIOPROD SRL**.

DOMENIUL: Procedura se aplică în activitatea de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal. Procedura se aplică, corespunzător competențelor, de către:

- personalul desemnat din cadrul Structurii de Tehnologia Informației;
- structura responsabilă cu protecția datelor personale;
- personalul extern care asigură mentenanța infrastructurii IT din cadrul firmei;
- angajaților **ALCOS BIOPROD SRL**.

TERMENI ȘI DEFINIȚII:

ANSPDCP = Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;

Codul numeric personal (CNP) = un număr semnificativ care individualizează în mod unic o persoană fizică, constituind un instrument de verificare a stării civile a

acesteia și de identificare în anumite sisteme informatice de către persoanele autorizate;

Date cu caracter personal = orice informații referitoare la o persoană fizică identificată sau identificabilă; o persoană identificabilă este acea persoană care poate fi identificată, direct sau indirect, în mod particular prin referire la un număr de identificare ori la unul sau la mai mulți factori specifici identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;

Date cu caracter personal cu funcție de identificare de aplicabilitate generală (date cu caracter special) = numere prin care se identifică o persoană fizică în anumite sisteme de evidență și care au aplicabilitate generală, cum ar fi: codul numeric personal, seria și numărul actului de identitate, numărul pașaportului, al permisului de conducere, numărul de asigurare socială sau de sănătate;

Date anonime - date care, datorită originii sau modalității specifice de prelucrare, nu pot fi asociate cu o persoană identificată sau identificabilă;

Operator - 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 prevazute în dreptul Uniunii sau în dreptul intern;

Persoană împuternicită de către operator - o persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, care prelucrează date cu caracter personal pe seama operatorului;

Responsabilul cu protecția datelor – persoana desemnată cu:

- Informarea și consilierea operatorului precum și a angajaților cu privire la obligațiile care le revin referitoare la protecția datelor;
- Monitorizarea respectării regulamentului GDPR și a politicilor operatorului în ceea ce privește protecția datelor cu caracter personal, inclusiv acțiunile de sensibilizare și de formare a personalului;
- Furnizarea de consiliere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;
- Cooperarea cu autoritatea de supraveghere;
- Asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare.

Prelucrarea datelor cu caracter personal - orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea către terți prin

transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

Stocarea - păstrarea pe orice fel de suport a datelor cu caracter personal culese, respectând în același timp protecția datelor cu caracter personal „începând cu momentul concepției și în mod implicit” (by design and by default);

Utilizator - orice persoană care acționează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.

1. CONDIȚII DE LEGITIMITATE

ALCOS BIOPROD SRL prelucrează datele cu caracter personal înregistrate în sistemele IT ale firmei, respectând prevederile legale în domeniu.

1.1 Referințe normative:

- a) Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare;
- b) Ordinul nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal;
- c) Decizia nr. 200 din 14 decembrie 2015 privind stabilirea cazurilor de prelucrare a datelor cu caracter personal pentru care nu este necesară notificarea, precum și pentru modificarea și abrogarea unor decizii;
- d) Ordinul Avocatului Poporului nr. 52 din 18/04/2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal;
- e) Decizia ANSPDCP nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video;
- f) Decizia ANSPDCP nr. 132 din 20/12/2011 privind condițiile prelucrării codului numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală;
- g) Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.**

1.2 Transparență

Procedură de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal este disponibilă ca anexă a Regulamentului de Ordine Interioară ALCOS BIOPROD SRL.

1.3 Revizuiți periodice

O revizuire periodică va fi întreprinsă anual sau ori de câte ori apar modificări legislative, de către structurile responsabile cu asigurarea securității și va reanaliza:

- îndeplinirea scopului declarant;
- posibile îmbunătățiri ale **Procedurii de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.**

2. Reguli Generale

Prin cerințe minime de securitate aplicate în cadrul **ALCOS BIOPROD SRL**, este avut în vedere un complex de măsuri tehnice, informatice, organizatorice, logistice, proceduri și politici de securitate prin care să se asigure nivelul minim de securitate prevăzut în art. 20 din Legea nr. 677/2001 și luând în considerare cerințele din legislația națională, deciziile ANSPDCP în acest domeniu și Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.

ALCOS BIOPROD SRL a adoptat măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat. În acest sens au fost desemnate, la nivelul **ALCOS BIOPROD SRL**, persoane responsabile cu respectarea dispozițiilor Legii nr.677/2001.

ALCOS BIOPROD SRL a luat măsuri de stocare în siguranță a informațiilor privind date cu caracter personal, astfel încât să fie asigurat un nivel adecvat de protecție și securitate, în sensul Legii 677/2001 al deciziilor ANSPDCP în acest domeniu și Regulamentul (UE) 2016/679.

Activitatea de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, este în responsabilitatea Responsabilului cu

Protecția Datelor cu Caracter Personal / Data Protection Officer, care este anunțat despre incidentul privind datele cu caracter personal în cel mai scurt timp.

Activitățile pe care le efectuează DPO sunt:

- ✓ Se documentează despre datele deținute în cazul repectiv;
- ✓ Se asigură că petentul are calitatea legală pentru a cere respectarea dreptului prevăzut de GDPR;
- ✓ Documentează baza legală a prelucrărilor de date implicate;
- ✓ Dispune măsurile necesare pentru elaborarea răspunsului / rezolvarea petiției respective, respective a incidentului semnalat privind datele cu caracter personal dacă acestea implică și alte operațiuni decât informarea;
- ✓ Elaborează răspunsul către petent;
- ✓ Asigură dialogul cu ANSPDCP și elaborează răspunsul / răspunsurile către ANSPDCP, respectând prevederile Regulamentul (UE) 2016/679 și ale legislației în vigoare;
- ✓ Aplică prevederile referitoare la activitatea de dialog cu petentul și cu ANSPDCP, împreună cu alte măsuri și prevederi aprobate în cadrul **ALCOS BIOPROD SRL** prin sistemul de proceduri de implementare a GDPR anexe la Regulamentul de Ordine Interioară **ALCOS BIOPROD SRL**;
- ✓ Se asigură de respectarea deciziilor, respectiv de aplicarea măsurilor legale prevăzute de GDPR.

3. Activitatea de răspuns la incidentele privind datele cu caracter personal, inclusiv în legătură cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

3.1. Timpul de raspuns la un incident semnalat / petiție / solicitare venită din partea persoanelor interesate, respectiv a persoanele fizice vizate de prelucrarea datelor cu caracter personal, conform legislației europene prin aplicarea Regulamentului nr. 679/2016

În conformitate cu Articolului 12, Alineatul 3 din Regulamentul nr. 679/2016: timpul maxim de răspuns la o petiție / solicitare / incident semnalat este de 30 de zile.

ALCOS BIOPROD SRL, ca operator, se obligă să furnizeze persoanei vizate informații privind acțiunile întreprinse în urma unei cereri fără întârzieri nejustificate și în orice caz în cel mult o lună de la primirea cererii.

Atunci când e necesar, din motive legate de complexitatea și volumul cererilor primite simultan, această perioadă poate fi prelungită până la două luni.

Chiar și în aceste condiții de prelungire, **ALCOS BIOPROD SRL** va informa persoana vizată de această prelungire tot în intervalul de o lună. Pentru cererile trimise în format electronic, informațiile vor fi furnizate în format electronic – acolo unde este posibil, cu excepția cazului în care persoana vizată solicită informațiile într-un alt format.

3.2. Persoanele îndreptățite să depună o plângere referitoare la prelucrarea datelor cu caracter personal în cadrul ALCOS BIOPROD SRL

Plângerile, sesizările și cererile pot fi depuse personal sau prin reprezentant, de către persoanele îndreptățite să depună o plângere referitoare la prelucrarea datelor cu caracter personal, cu menționarea obligatorie a numelui, prenumelui, adresei de domiciliu sau de corespondență și a semnăturii persoanei fizice.

În cazul în care plângerile, sesizările și cererile se depun prin reprezentant, sunt obligatorii datele de identificare ale acestuia (nume, prenume, adresă de domiciliu sau de corespondență/denumire, sediu și adresă de corespondență) și anexarea împuternicirii semnate de persoana interesată.

În cazul plângerilor, sesizărilor și cererilor transmise prin poștă electronică sau on-line, este obligatorie menționarea unei adrese valabile de poștă electronică pentru contactarea petiționarului.

Toate plângerile, sesizările și cererile depuse în cadrul ALCOS BIOPROD SRL de către persoanele fizice interesate, vor fi înregistrate obligatoriu cu număr de înregistrare în registrul de intrare – ieșire a documentelor în cadrul ALCOS BIOPROD SRL.

Plângerile, sesizările și cererile în care nu se precizează datele de identificare ale petiționarului, respectiv, nume, prenume, adresă de domiciliu sau corespondență, sunt considerate anonime. Acestea nu se înregistrează, se clasează cu această mențiune în registrul de intrare – ieșire a documentelor în cadrul **ALCOS BIOPROD SRL**.

În cazul în care un petiționar adresează mai multe petiții / sesizări, sesizând aceeași problemă, respectiv același incident, acestea se conexează, petiționarul urmând să primească un singur răspuns care trebuie să facă referire la toate petițiile / sesizările depuse de către petiționar.

3.3. Drepturile persoanelor fizice vizate de prelucrarea datelor cu caracter personal

Regulamentul (UE) 2016/679 privind protecția persoanelor fizice (denumit și GDPR) vine cu unele drepturi noi pentru indivizi și consolidează unele dintre drepturile care existau deja în Legislația Europeană.

Astfel, GDPR oferă persoanelor fizice vizate de prelucrarea datelor cu caracter personal următoarele drepturi generale:

- ✓ dreptul de a fi informat;
- ✓ dreptul de acces;
- ✓ dreptul la rectificare;
- ✓ dreptul de ștergere;
- ✓ dreptul de a restricționa procesarea;
- ✓ dreptul la portabilitatea datelor;
- ✓ dreptul la obiect (sau dreptul de a ridica obiecții);
- ✓ drepturi legate de luarea de decizii automatizate și de profilare.

4. Prelucrarea și protecția datelor

Prelucrarea datelor cu caracter personal în cadrul **ALCOS BIOPROD SRL** se realizează cu respectarea cerințelor legale și în condiții care să asigure securitatea, confidențialitatea și respectarea drepturilor generale ale persoanelor vizate prezentate mai sus, amănunțit în această procedură, respectiv: dreptul de a fi informat, dreptul de acces, dreptul la rectificare, dreptul de ștergere, dreptul de a restricționa procesarea, dreptul la portabilitatea datelor, dreptul la obiect (sau dreptul de a ridica obiecții), drepturi legate de luarea de decizii automatizate și de profilare.

Procedura specifică de acces, prelucrare și protecție a datelor este disponibilă ca anexă a Regulamentului de Ordine Interioară **ALCOS BIOPROD SRL**.

5. GARANTAREA DREPTURILOR PERSOANEI VIZATE

ALCOS BIOPROD SRL garantează că asigură respectarea drepturilor ce revin persoanelor vizate, conform legii. Toate persoanele implicate în activitatea de colectare a datelor personale și cele responsabile de administrarea imaginilor filmate, vor respecta **Procedura specifică de acces, prelucrare și protecție a datelor cu caracter personal**.

5.1. Exercițarea drepturilor de acces, intervenție și opoziție

Pe întreaga perioadă de stocare a datelor cu caracter personal, persoanele vizate au dreptul de acces la datele personale care le privesc, de a solicita intervenția (ștergere/actualizare/rectificare/anonimizare) sau de a se opune prelucrărilor, conform legii. Orice cerere de a accesa, rectifica, bloca și/sau șterge date cu caracter personal ar trebui să fie adresată **ALCOS BIOPROD SRL**, iar o copie a acesteia trebuie trimisă către Responsabilul cu Protecția Datelor Personale.

Există posibilitatea refuzării dreptului de acces în situația în care se aplică excepțiile prevăzute de lege. Necesitatea de a restricționa accesul se poate impune și în cazul în care există obligația de a proteja drepturile și libertățile unor terțe persoane.

6. Activitatea de răspuns la incidentele privind datele cu caracter personal, în legătură cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

Conform **Articolului 33** din GDPR va fi obligatoriu ca o organizație cu rol de operator să raporteze autorității sale de supraveghere orice breșă de securitate a datelor personale în termen de 72 de ore de la conștientizarea acesteia. Dacă această cerință nu este îndeplinită, raportul final trebuie însoțit de o explicație a întârzierii. Notificarea trebuie să includă informații specifice, inclusiv o descriere a măsurilor luate pentru a soluționa breșa și pentru a atenua posibilele efecte secundare.

În cazul în care breșa poate avea ca rezultat un risc ridicat pentru drepturile și libertățile persoanelor fizice, indivizii înșiși trebuie să fie contactați „fără întârzieri nejustificate”. Acest contact nu va fi necesar dacă există măsuri de protecție adecvate – în esență, criptare – pentru a elimina pericolul pentru persoanele vizate.

În **Articolul 33 – Notificarea unei încălcări a datelor cu caracter personal către autoritatea de supraveghere**, se specifică foarte clar că:

- Raportarea în situația apariției unor breșe de securitate este obligatorie pentru orice operator de date personale;
- Operatorii trebuie să raporteze către autorităților de supraveghere competente orice încălcare a condițiilor de siguranță fără întârzieri nejustificate;
- Dacă este posibil, nu mai târziu de 72 de ore de la prima conștientizare;
- Dacă raportarea nu este făcută în termen de 72 de ore, trebuie furnizată o justificare a întârzierii;

- Nu este necesară notificarea cazurilor în care încălcarea este «puțin probabil să ducă la un risc pentru drepturile și libertățile» persoanelor vizate;
- Dacă breșa de securitate este constatată de către un procesator de date, acesta trebuie să notifice operatorul cu care colaborează fără întârzieri nejustificate.

6.1. Informații incluse în notificarea unei breșe de securitate

Elementele esențiale care trebuie să se regăsească într-o notificare se referă la:

- natura încălcării datelor cu caracter personal;
- categoriile și numărul aproximativ al persoanelor implicate;
- categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
- numele și datele de contact ale responsabilului cu protecția datelor (în cazul în care organizația dvs. dispune de unul) sau orice alt punct de contact de unde pot fi obținute mai multe informații;
- descriere a consecințelor probabile ale încălcării datelor cu caracter personal;
- descriere a măsurilor luate sau propuse a fi luate pentru a face față încălcării datelor cu caracter personal dacă este cazul, o descriere a măsurilor luate pentru a atenua eventualele efecte adverse.

6.2. Situații în care nu se notifică persoanele vizate

În **Articolul 34: Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal, Alineatul 3**, regulamentul stipulează că informarea persoanei vizate nu este necesară în cazul în care este îndeplinită oricare dintre următoarele condiții:

- ✓ operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar acestea 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;
- ✓ operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate nu mai este susceptibil să se materializeze;
- ✓ informarea 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.

6.3 Ghidul recomandărilor legate de anunțarea breșelor de Securitate

De pe site-ul oficial al [Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal \(ANSPDCP\)](#) poate fi descărcat "**Ghidul privind notificarea încălcărilor de securitate**", un instrument deosebit de util în implementarea condițiilor impuse de GDPR, elaborate de Grupul de Lucru, Articolul 29.

Tot de pe site-ul Autorității Naționale pot fi accesate și consultate formularele utilizate deja în notificarea breșelor de securitate conform legislației actuale.

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.