GDPR · ARTICOLUL 28

Acord de Prelucrare a Datelor (DPA)

Acord între Operatorul de date (Client) și NexusMed Medicina Muncii SRL (Persoană Împuternicită), conform Regulamentului (UE) 2016/679 (GDPR).

DOCUMENT	Data Processing Agreement (DPA)
VERSIUNE	1.0
ULTIMA ACTUALIZARE	15.05.2026
GENERAT LA	07.11.2026 15:40
PROCESOR	NexusMed Medicina Muncii SRL
CUI PROCESOR	RO00000000

Acest document este parte integrantă din contractul de servicii încheiat cu NexusMed Medicina Muncii SRL. Pentru aplicabilitate, completați câmpurile marcate cu **[●]** și semnați.

Important: Acest Acord de Prelucrare a Datelor (DPA) face parte integrantă din contractul de servicii încheiat între Client (Operator de date) și NexusMed Medicina Muncii SRL (Persoană Împuternicită). DPA-ul reglementează condițiile prelucrării datelor cu caracter personal conform Art. 28 GDPR.

1 Părțile contractante

Operator de date (Controller)

DENUMIRE	[DENUMIRE CLIENT / COMPANIE]
CUI	[●]
ADRESA	[●]
REPREZENTANT LEGAL	[●]
EMAIL	[●]

Persoana Împuternicită (Processor)

DENUMIRE	NexusMed Medicina Muncii SRL
CUI	RO00000000
REG. COMERȚULUI	J00/0000/2025
SEDIU	Str. Exemplu nr. 1, București, România
EMAIL CONTACT	contact@nexuxmed.ro
DPO	Responsabil GDPR – gdpr@nexuxmed.ro

2 Obiectul acordului

Prezentul DPA reglementează condițiile în care **Processorul** (NexusMed Medicina Muncii SRL) prelucrează date cu caracter personal **în numele Operatorului**, în cadrul utilizării aplicației web NexusMed.

Acordul se aplică pe toată durata utilizării serviciilor și se completează cu prevederile contractului principal de prestări servicii.

3 Natura și scopul prelucrării

Natura operațiunilor de prelucrare

- Colectare
- Stocare
- Organizare și structurare
- Consultare și extragere
- Utilizare în cadrul fluxurilor aplicației
- Modificare și actualizare
- Arhivare
- Ștergere sau distrugere
- Transmitere (doar către sub-procesatori autorizați și conform indicațiilor Operatorului)

Scopul prelucrării

- Gestionarea activității medicale / medicina muncii
- Administrarea pacienților și angajaților
- Generarea documentelor medicale (fișe aptitudine, dosare, rapoarte)
- Programarea și evidența serviciilor medicale
- Îndeplinirea obligațiilor legale ale Operatorului

4 Tipuri de date prelucrate

Date de identificare

- Nume, prenume
- Cod Numeric Personal (CNP)
- Serie și număr carte de identitate
- Adresa de domiciliu

Date de contact

- Număr de telefon
- Adresa de email

Date profesionale

- Funcția / ocupația
- Angajatorul
- Locul de muncă

Date speciale (sensibile) – Art. 9 GDPR

- Date medicale
- Rezultate analize și investigații
- Fișe medicale și antecedente
- Concluzii medicale și aviz de aptitudine

5 Categorii de persoane vizate

- Pacienți / persoane examinate
- Angajați ai companiilor cliente
- Colaboratori medicali
- Utilizatori ai aplicației (operatori interni)

6 Durata prelucrării

Datele sunt prelucrate pe durata contractului principal încheiat între părți și ulterior conform obligațiilor legale aplicabile (în special **arhivarea fișelor medicale conform legislației medicale române**).

La încetarea contractului, datele se șterg sau se returnează Operatorului conform Secțiunii 13.

7 Obligațiile Processorului (NexusMed Medicina Muncii SRL)

Securitate tehnică

- Criptare a transmisiilor de date (HTTPS / TLS)
- Parole hashuite cu algoritmi siguri (bcrypt / argon2)
- Protecție împotriva accesului neautorizat
- Backup periodic al datelor
- Recuperare în caz de dezastru

Securitate organizatorică

- Acces limitat pe roluri (RBAC – Role Based Access Control)
- Loguri complete de acces și audit
- Politici interne de securitate
- Instruire periodică a personalului cu acces la date
- Acorduri de confidențialitate cu angajații și colaboratorii

Securitate aplicativă (Laravel-specific)

- Protecție CSRF (Cross-Site Request Forgery) pe toate formularele
- Validare strictă a inputului utilizatorului
- Prevenire SQL Injection prin Eloquent ORM și prepared statements
- Protecție XSS (Cross-Site Scripting) prin escape automat în template-uri Blade
- Hash-uire bcrypt 12 rounds pentru parole
- Captcha la autentificare împotriva atacurilor automate
- Sesiuni securizate cu rotire periodică a token-urilor

8 Sub-procesatori

Processorul poate utiliza sub-procesatori pentru îndeplinirea obligațiilor sale, în următoarele categorii:

- **Hosting** – furnizori VPS / cloud, situați în UE
- **Servicii email** – pentru notificări transactționale
- **Servicii backup** – copii de siguranță offsite
- **Servicii de monitoring** – uptime, performanță

Toți sub-procesatorii respectă **GDPR** și sunt obligați contractual să asigure același nivel de protecție a datelor. Lista actuală a sub-procesatorilor poate fi furnizată la cerere.

9 Transferuri internaționale

Datele **NU sunt transferate în afara Uniunii Europene**, cu excepția situațiilor unde există garanții adecvate prevăzute de GDPR (clauze SCC, decizii de adecvare, reguli corporative obligatorii).

10 Drepturile persoanelor vizate

Processorul asistă Operatorul, în măsura posibilităților tehnice, pentru a răspunde solicitărilor persoanelor vizate privind exercitarea drepturilor:

- Drept de acces (Art. 15 GDPR)
- Drept de rectificare (Art. 16 GDPR)
- Drept de ștergere – „dreptul de a fi uitat" (Art. 17 GDPR)
- Drept de restricționare (Art. 18 GDPR)
- Drept de portabilitate (Art. 20 GDPR)
- Drept de opoziție (Art. 21 GDPR)
- Drept de a nu fi supus unei decizii automate (Art. 22 GDPR)

11 Notificarea incidentelor de securitate

În cazul identificării unui incident de securitate care afectează datele Operatorului, Processorul:

- Va notifica Operatorul în **maxim 72 de ore** de la identificare
- Va furniza toate informațiile relevante despre incident
- Va coopera cu Operatorul pentru investigare și remediere
- Va sprijini Operatorul în notificarea autorității de supraveghere (ANSPDCP), dacă este cazul

12 Confidențialitate

Toate persoanele care au acces la datele Operatorului în cadrul prestării serviciilor sunt obligate contractual la confidențialitate, atât pe durata contractului, cât și după încetarea acestuia.

13 Returnarea / ștergerea datelor

La încetarea contractului, la cererea Operatorului, Processorul:

- Returnează toate datele într-un format structurat și utilizabil (CSV / Excel / SQL dump)
- Șterge toate copiile datelor de pe serverele sale (cu excepția cazurilor în care păstrarea este obligată legal)
- Furnizează o confirmare scrisă a ștergerii

Termen: maxim 30 de zile de la solicitare, sau o perioadă mai lungă convenită în scris.

14 Drept de audit

Operatorul are dreptul de a audita modul în care Processorul prelucrează datele, prin:

- Solicitarea de informații și documente referitoare la măsurile de securitate implementate
- Inspecții la sediul Processorului, anunțate cu minim 30 zile în avans
- Auditare prin terți independenți autorizați (cu acord prealabil al Processorului)

Costurile auditului sunt suportate de Operator, cu excepția cazului în care auditul descoperă încălcări semnificative ale prezentului DPA.

15 Răspundere

Fiecare parte răspunde, conform GDPR, pentru încălcările care îi sunt imputabile. Răspunderea este reglementată de prevederile contractului principal și de Art. 82 GDPR.

16 Legea aplicabilă

Prezentul acord este guvernat de:

- Legislația din **România**
- Regulamentul (UE) 2016/679 (**GDPR**)
- Legea nr. **190/2018** privind măsuri de punere în aplicare a GDPR

17 Semnături

Pentru încheierea oficială a prezentului DPA, completați câmpurile marcate cu **[●]** și semnați. Semnătura electronică calificată este acceptată conform legislației aplicabile.

OPERATOR (Client)	PROCESOR (NexusMed Medicina Muncii SRL)
NUME ȘI PRENUME:	**NUME ȘI PRENUME:**
FUNCȚIE:	**FUNCȚIE:**
DATA:	**DATA:**
SEMNĂTURA ȘI ȘTAMPILA:	**SEMNĂTURA ȘI ȘTAMPILA:**

Versiune document: 1.0 · **Data ultimei actualizări:** 15.05.2026 · **Generat:** 07.11.2026 15:40