DataLex

GHID PRACTIC · EDIȚIA IULIE 2026

Pregătirea companiei pentru Legea nr. 195/2024

Cei 6 pași prin care compania dvs. ajunge la conformitate cu noua lege a protecției datelor cu caracter personal, înainte de intrarea ei în vigoare. Cu întrebări de audit, liste de verificare și calendarul recomandat.

23.08.2026
data intrării în vigoare a legii

până la 2%
din cifra de afaceri anuală sau 2 mil. MDL, sancțiunea maximă (art. 88)

2-4 luni
durata unei implementări corecte

6 pași
de la inventarierea datelor până la instruirea angajaților

www.datalex.md · contact@datalex.md · 079 248 248

Material informativ gratuit

De ce contează și cui i se aplică

Pe 23 august 2026 intră în vigoare Legea nr. 195/2024 privind protecția datelor cu caracter personal, care înlocuiește Legea 133/2011 și aliniază Republica Moldova la standardul european GDPR.

Legea se aplică practic oricărei companii

Dacă aveți cel puțin un angajat sau un client persoană fizică, prelucrați date cu caracter personal: dosare de personal, CV-uri, state de plată, liste de clienți, contracte, corespondență, imagini video. Mărimea companiei nu contează; volumul obligațiilor diferă, obligația în sine nu.

Ce riscați dacă nu faceți nimic

- Sancțiuni pe două niveluri (art. 88): până la 1.000.000 MDL sau 1% din cifra de afaceri anuală pentru încălcări obișnuite, și până la 2.000.000 MDL sau 2% din cifra de afaceri anuală pentru încălcări grave; se aplică suma mai mare.
- Controale și prescripții din partea CNPDCP (Centrul Național pentru Protecția Datelor cu Caracter Personal), inclusiv în urma plângerilor depuse de angajați sau clienți.
- Cereri ale persoanelor vizate la care nu veți putea răspunde: legea vă dă cel mult o lună pentru fiecare cerere de acces, rectificare sau ștergere.
- Parteneri și clienți corporativi, mai ales din UE, care cer dovada conformității înainte de a semna un contract.

Cei 6 pași din acest ghid

1. Inventarierea datelor · **2.** Harta prelucrărilor și registrul (art. 30) · **3.** Gap-analiza · **4.** Documentele obligatorii · **5.** Securitatea IT și furnizorii · **6.** Instruirea și reacția la incidente

De ce să începeți acum: o implementare corectă durează 2-4 luni. Companiile care amână ajung să facă totul superficial, sub presiune, sau să plătească tarife de urgență. Începutul devreme înseamnă costuri mai mici și procese așezate.

1 PASUL 1 · APROX. 2-3 SĂPTĂMÂNI

Inventariați datele pe care le aveți

Nu puteți proteja ce nu știți că există. Primul pas este un audit intern: ce date personale dețineți, unde stau, cine le atinge și de ce.

Întrebările de pus în fiecare departament

Resurse umane

- Ce conțin dosarele de personal și cât timp le păstrăm?
- Păstrăm CV-uri ale candidaților respinși? De când?
- Cine are acces la dosare și la datele de sănătate (concedii medicale)?

Contabilitate

- Ce date de angajați și persoane fizice apar în state de plată și contracte?
- Unde se țin: program local, cloud, hârtie?
- Se transmit date către bănci, CNAS, SFS? Pe ce cale?

Vânzări și marketing

- Ce baze de clienți și liste de contacte avem și de unde provin?
- Trimitem newslettere? Avem consimțământul fiecărui destinatar?
- Site-ul colectează date prin formulare sau cookie-uri?

IT și administrativ

- Pe ce servere și în ce servicii cloud stau datele?
- Avem supraveghere video? Este semnalizată?
- Ce se întâmplă cu conturile angajaților care pleacă?

Greșeala frecventă: inventarul se face doar pe sisteme electronice și se uită hârtia: dosare din dulapuri, arhive, registre de vizitatori, copii ale buletinelor. Legea nu face diferența între digital și hârtie.

2 PASUL 2 · APROX. 2-3 SĂPTĂMÂNI

Întocmiți harta prelucrărilor și registrul (art. 30)

Rezultatele auditului se organizează în registrul activităților de prelucrare, documentul pe care CNPDCP îl cere primul la orice control. Lipsa lui este, în sine, o încălcare.

Ce coloane trebuie să aibă registrul

Element	Exemplu concret
Procesul / scopul prelucrării	evidența personalului; calculul salariilor; marketing direct
Categoriile de persoane vizate	angajați, candidați, clienți, vizitatori
Categoriile de date	identificare, contact, financiare, date de sănătate
Temeiul juridic	contract de muncă, obligație legală, consimțământ, interes legitim
Destinatarii	bănci, CNAS, contabilitate externalizată, furnizori IT
Transferuri în afara țării	cloud cu servere în UE/SUA, cu garanțiile aplicabile
Termenul de păstrare	dosar personal: conform legislației de arhivare; CV respins: 6-12 luni
Măsurile de securitate	acces restricționat, criptare, dulap încuiat

Regula de aur a hărții

Pentru fiecare proces trebuie să puteți răspunde într-o frază: ce date, despre cine, de ce, pe ce temei, cine le vede, unde ajung și când se șterg. Dacă la oricare dintre aceste întrebări răspunsul e „nu știm", ați găsit exact locul unde trebuie lucrat.

3 PASUL 3 · APROX. 1-2 SĂPTĂMÂNI

Faceți gap-analiza: unde nu corespundeți legii

Comparați situația reală cu cerințele legii. Fiecare răspuns „nu" de mai jos este un punct din planul dvs. de acțiuni, cu responsabil și termen.

Lista de verificare rapidă

- [ ] Fiecare prelucrare are un temei juridic clar (art. 6): contract, obligație legală, consimțământ valabil sau interes legitim documentat?
- [ ] Persoanele vizate sunt informate ce se întâmplă cu datele lor (art. 13-14): angajați, clienți, candidați, vizitatori?
- [ ] Există o procedură prin care puteți răspunde în cel mult o lună la o cerere de acces, rectificare sau ștergere (art. 12, 15-22)?
- [ ] Consimțămintele sunt libere, specifice și demonstrabile, nu bife pre-completate sau acorduri „la pachet" (art. 7)?
- [ ] Datele au termene de păstrare definite și există un mecanism real de ștergere la expirare (art. 5)?
- [ ] Contractele cu furnizorii care ating date (contabilitate externă, IT, hosting) conțin clauzele cerute de art. 28?
- [ ] Transferurile de date în afara Republicii Moldova sunt identificate și au un temei legal (art. 44-49)?
- [ ] Știți dacă aveți obligația de a desemna un responsabil pentru protecția datelor (art. 37-39)?
- [ ] Prelucrările cu risc ridicat (monitorizare, date de sănătate pe scară largă) au evaluare de impact, DPIA?
- [ ] Există o procedură de reacție la incidente de securitate, cu notificarea CNPDCP (art. 33-34)?

> **Prioritizați după risc:** nu totul se rezolvă deodată. Începeți cu prelucrările care ating multe persoane sau date sensibile: dosarele de personal, datele de sănătate, marketingul fără consimțământ, supravegherea video.

4 PASUL 4 · APROX. 3-5 SĂPTĂMÂNI

Elaborați documentele obligatorii

Documentele transformă practica în conformitate demonstrabilă. Setul minim pentru o companie tipică:

Documentul	Ce acoperă
Politica internă de protecție a datelor	regulile generale ale companiei: principii, roluri, responsabilități
Registrul activităților de prelucrare	harta completă de la Pasul 2, ținută la zi (art. 30)
Note de informare	pentru angajați, clienți, candidați și vizitatori (art. 13-14)
Formulare de consimțământ	marketing, categorii speciale, alte situații care îl cer (art. 6-7)
Politica de păstrare și distrugere	termene pe categorii de date și modul de ștergere sau anonimizare
Procedura de răspuns la cereri	cine primește, cine verifică identitatea, cine răspunde, în ce termen
Regulamentul de reacție la incidente	detectare, evaluare, notificarea CNPDCP și a persoanelor, registrul incidentelor
Contracte DPA și clauze pentru furnizori	acorduri de prelucrare cu terții care ating date (art. 28), NDA-uri

Pentru site și aplicații se adaugă Politica de confidențialitate publică, Politica de cookie-uri și bannerul de consimțământ.

> **Atenție la șabloane:** documentele copiate de pe internet, scrise pentru GDPR european sau pentru altă companie, nu descriu realitatea dvs. La control, diferența dintre document și practică se vede imediat și agravează situația în loc s-o ajute.

5 PASUL 5 · ÎN PARALEL CU PASUL 4

Securizați infrastructura IT și furnizorii

Datele nu stau în dosare, stau pe servere. Legea cere măsuri tehnice concrete (art. 32), nu doar politici pe hârtie. Lista de verificare pentru echipa IT sau furnizorul dvs. extern:

Accesul la date

- [ ] Conturi nominale pentru fiecare angajat; nicio parolă comună, niciun bilețel lipit de monitor.
- [ ] Drepturi de acces pe roluri: fiecare vede doar ce îi trebuie pentru munca lui.
- [ ] Procedură de retragere a accesului în ziua plecării unui angajat.

Protecția tehnică

- [ ] Criptarea discurilor pe laptopuri și a canalelor de transmitere (HTTPS, VPN).
- [ ] Copii de rezervă testate periodic, protejate la fel de strict ca datele originale.
- [ ] Jurnalizare: cine, când și ce date a accesat; fără loguri nu puteți nici demonstra conformitatea, nici investiga un incident.
- [ ] Actualizări de securitate aplicate la timp; antivirus și autentificare în doi pași unde e posibil.

Furnizorii și transferurile

- [ ] Inventarul serviciilor externe care ating date: hosting, CRM, e-mail, contabilitate externalizată.
- [ ] Contract conform art. 28 cu fiecare; furnizorul este persoană împuternicită, dar răspunderea rămâne și a dvs.
- [ ] Pentru serviciile cu servere în afara țării: identificați țara și temeiul legal al transferului (art. 44-49).

> **Bonus de eficiență:** ștergeți datele expirate, reduceți numărul de copii, separați sistemele. Mai puține date înseamnă risc mai mic, costuri mai mici și sisteme mai rapide.

6 PASUL 6 · APROX. 1-2 SĂPTĂMÂNI

Instruiți angajații și pregătiți reacția la incidente

Cele mai multe incidente pleacă de la oameni, nu de la tehnică: un e-mail trimis greșit, o parolă împrumutată, un dosar uitat pe birou. Documentele fără instruire rămân hârtie.

Ce trebuie să acopere instruirea

- [ ] Ce sunt datele personale și ce prelucrează concret compania dvs.
- [ ] Regulile zilnice: birou curat, ecran blocat, ce se trimite și ce nu se trimite pe e-mail sau messenger.
- [ ] Cum se recunoaște o cerere a unei persoane vizate și cui i se predă imediat.
- [ ] Cum se recunoaște un incident de securitate și cui i se raportează, în aceeași zi.
- [ ] Confirmare sub semnătură: instruirea nedocumentată nu există la control.

Procedura de incident, în 4 timpi

Timp	Acțiune
1. Detectare	angajatul raportează imediat responsabilului desemnat; se oprește extinderea incidentului
2. Evaluare	ce date, câte persoane, ce risc pentru ele; totul se documentează în registrul de incidente
3. Notificare	CNPDCP este notificat în termenul legal (art. 33); la risc ridicat se informează și persoanele vizate (art. 34)
4. Corectare	se elimină cauza, se actualizează măsurile și instruirea; concluziile intră în registru

Greșeala care costă cel mai mult: ascunderea incidentului. Sancțiunea pentru nenotificare se adaugă la sancțiunea pentru încălcarea propriu-zisă, iar la control istoricul iese oricum la iveală.

Calendarul recomandat și echipa proiectului

Pentru o companie tipică, drumul complet durează 2-4 luni. Orientativ, pe săptămâni:

Perioada	Etapa	Rezultatul
Săpt. 1-3	Inventarierea datelor (Pasul 1)	lista completă a datelor și sistemelor
Săpt. 3-6	Harta prelucrărilor și registrul (Pasul 2)	registrul art. 30, prima versiune
Săpt. 6-8	Gap-analiza (Pasul 3)	plan de acțiuni prioritizat, cu responsabili
Săpt. 8-13	Documente + măsuri IT (Pașii 4-5, în paralel)	setul de documente semnat; cerințele tehnice implementate
Săpt. 13-15	Instruirea și predarea (Pasul 6)	angajați instruiți sub semnătură; dosarul de conformitate complet

Cine face parte din echipa proiectului

- **Conducerea**: decide, alocă resurse și dă greutate proiectului în fața echipei.
- **Juridic** (intern sau extern): conduce metodologic, redactează documentele.
- **HR / resurse umane**: dosarele de personal, candidații, instruirea.
- **Contabilitate**: statele de plată, schimburile cu instituțiile de stat.
- **IT**: măsurile tehnice, accesele, furnizorii, copiile de rezervă.
- **Șefii de subdiviziuni**: cunosc fluxurile reale de date din teren.

Decizia despre DPO

Responsabilul pentru protecția datelor este obligatoriu doar în cazurile prevăzute la art. 37-39, de exemplu la prelucrări pe scară largă sau de categorii speciale. Evaluați obligația la Pasul 3; dacă e necesar, funcția poate fi externalizată, fără angajare separată.

Lista de verificare finală

Sunteți pregătiți când puteți bifa fiecare rând de mai jos:

- [ ] Știm ce date personale avem, unde stau și cine are acces la ele.
- [ ] Registrul activităților de prelucrare există și este actualizat (art. 30).
- [ ] Fiecare prelucrare are temei juridic; consimțămintele sunt demonstrabile.
- [ ] Angajații, clienții și candidații au primit notele de informare.
- [ ] Putem răspunde în cel mult o lună la orice cerere a unei persoane vizate.
- [ ] Termenele de păstrare sunt definite și ștergerea chiar se întâmplă.
- [ ] Furnizorii care ating date au contracte conform art. 28; transferurile externe au temei legal.
- [ ] Măsurile tehnice (accese, criptare, backup, loguri) sunt implementate și verificate.
- [ ] Procedura de incidente există, iar echipa știe pe cine sună în prima oră.
- [ ] Angajații au fost instruiți și au semnat; decizia privind DPO este documentată.

Vreți să parcurgeți acești pași cu un partener alături?

DataLex oferă exact acest drum, de la audit până la dosarul complet de conformitate: Pachetul STARTER de la 350 € și Pachetul COMPLET, cu DPO extern și suport continuu, de la 500 €. Prima consultație este gratuită: ne uitați peste situația dvs. și primiți un plan concret, cu termene, indiferent dacă lucrăm apoi împreună.

TELEFON	E-MAIL	SITE	PROGRAM
079 248 248	contact@datalex.md	www.datalex.md	Luni - Vineri, 9:00 - 18:00