Frandeș
LAW

Bd. Timișoara nr. 26, Plaza Romania Offices
Et. 1, birourile 115-116, Sector 6, 061344, București
T: +40 746 426 538
E: office@frandes.law
W: www.frandes.law

PROPRIETATE INTELECTUALĂ, TEHNOLOGIE ȘI PROTECȚIA DATELOR · 13 NOIEMBRIE 2026

Contează, de fapt, mărimea firmei? GDPR, obligațiile angajatorilor și practica recentă a ANSPDCP

Despre obligațiile care nu depind de numărul de salariați, regimul sancționator și amenzile aplicate în ultimele 12 luni

Proprietate intelectuală, tehnologie și protecția datelor · 13 noiembrie 2026

O societate cu un singur angajat sau un magazin de cartier nu este scutită de regulile privind protecția datelor. GDPR nu distinge, ca regulă, după numărul de salariați.

Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (GDPR) se aplică oricărui operator stabilit în Uniunea Europeană, indiferent de forma juridică, cifra de afaceri sau efectivul de personal. Operatorul este entitatea care decide de ce și cum sunt colectate și folosite datele cu caracter personal. Prin urmare, GDPR se aplică tuturor societăților din România, oricât de mici sau de mari ar fi.

În dreptul intern, Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului instituie reguli speciale privind prelucrarea codului numeric personal și monitorizarea salariaților. Și ea se aplică oricărui angajator.

1. Obligațiile comune tuturor operatorilor

Nucleul obligațiilor este același pentru orice operator. Fiecare prelucrare de date trebuie să aibă un temei de legalitate. Persoanele vizate, ale căror date sunt prelucrate, trebuie informate, iar cererile pe care le adresează trebuie soluționate în termen de o lună. Cu persoanele împuternicite se încheie contracte. Prelucrarea trebuie să fie sigură, iar încălcările de securitate se notifică Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), dacă este posibil, în cel mult 72 de ore.

Diferențierea după dimensiunea întreprinderii poate apărea doar în privința obligațiilor de mai jos. Și acolo, în realitate, apare într-un singur punct.

2. Ce depinde de numărul de salariați și ce nu

a) Evidența activităților de prelucrare. Este un document scris, în format fizic sau digital, prin care organizația mapează și inventariază toate procesele în care colectează, folosește, stochează sau transmite date cu caracter personal. Pentru operatorii cu 250 de angajați sau mai mult, evidența este obligatorie. Pentru cei cu sub 250 de angajați, Regulamentul prevede o derogare, la art. 30 alin. (5), dar în practică se interpretează că obligația este valabilă și pentru ei. Este **singura obligație care distinge după numărul de salariați**.

b) Desemnarea responsabilului cu protecția datelor (DPO – Data Protection Officer). Desemnarea este obligatorie, oricare ar fi dimensiunea operatorului, dacă activitățile sale principale constau în monitorizarea periodică și sistematică pe scară largă sau în prelucrarea pe scară largă a categoriilor speciale de date. Pentru societățile de pază și supraveghere video, de exemplu, monitorizarea este activitatea principală. La fel, companiile de telecomunicații urmăresc traficul, geolocația prin relee GSM, istoricul apelurilor și metadatele de comunicații. Aplicațiile de transport urmăresc pe scară largă locația GPS, traseul în timp real și tiparele de deplasare ale clienților și șoferilor. Sistemele de profilare pentru publicitate online targetată fac același lucru. Toate realizează o urmărire continuă, organizată și extinsă a comportamentului sau a acțiunilor persoanelor.

c) Prelucrarea codului numeric personal. Orice angajator care înregistrează și prelucrează CNP-urile angajaților trebuie să respecte cerințe de securitate, confidențialitate, instruire și termene stricte de stocare. Dacă o societate colectează sau prelucrează CNP-ul clienților ori al altor terți în temeiul interesului legitim, o poate face numai cu măsuri tehnice și organizatorice speciale și **numai dacă își desemnează un DPO**, potrivit art. 4 alin. (2) din Legea nr. 190/2018. Exemplul tipic este furnizorul de servicii care cere CNP-ul clienților pentru a-și recupera mai ușor o datorie, fără să aibă o obligație legală directă în acest sens. Regimul este același pentru toți operatorii.

d) Monitorizarea salariaților prin mijloace electronice sau video. Potrivit art. 5 din Legea nr. 190/2018, monitorizarea este permisă numai dacă sunt îndeplinite cumulativ cinci condiții: un interes legitim temeinic justificat și prevalent, informarea prealabilă completă și explicită a salariaților, consultarea sindicatului sau a reprezentanților salariaților, ineficiența dovedită a mijloacelor mai puțin intruzive și o stocare proporțională, de cel mult 30 de zile, cu excepțiile prevăzute de lege. Condițiile nu diferă după dimensiunea angajatorului.

e) Evaluarea impactului asupra protecției datelor. Este obligatorie înaintea prelucrărilor susceptibile să genereze un risc ridicat, oricare ar fi dimensiunea operatorului.

> **Concluzia practică.** Dimensiunea întreprinderii nu exonerează de răspundere. Poate scuti, cel mult, de o singură obligație documentară, iar condițiile acestei scutiri sunt rareori întrunite.

3. Regimul sancționator

Sancțiunile contravenționale principale pe care le aplică ANSPDCP sunt avertismentul și amenda. În completare sau separat, autoritatea poate dispune măsuri corective, inclusiv limitarea sau interzicerea prelucrării.

Pentru întreprinderi, plafonul amenzii depinde de natura încălcării.

a) Obligațiile operatorului și ale persoanei împuternicite. Potrivit art. 83 alin. (4) GDPR, amenda poate ajunge la 10.000.000 EUR sau la 2% din cifra de afaceri mondială anuală a exercițiului financiar precedent, luându-se în calcul valoarea cea mai mare.

b) Principiile prelucrării și drepturile persoanelor vizate. Potrivit art. 83 alin. (5) GDPR, încălcarea principiilor prelucrării, a regulilor privind temeiul de legalitate, consimțământul și categoriile speciale de date, a drepturilor persoanelor vizate sau a regulilor privind transferurile internaționale se sancționează cu amendă de până la 20.000.000 EUR sau 4% din cifra de afaceri mondială anuală, luându-se în calcul valoarea cea mai mare.

c) Nerespectarea unui ordin al autorității de supraveghere. Potrivit art. 83 alin. (6) GDPR, se aplică același plafon: până la 20.000.000 EUR sau 4% din cifra de afaceri mondială anuală.

Pentru autoritățile și organismele publice, art. 14 din Legea nr. 190/2018 prevede amenzi între 10.000 și 100.000 lei, respectiv între 10.000 și 200.000 lei, după natura încălcării.

La individualizarea amenzii se au în vedere, între altele, natura, gravitatea și durata încălcării, caracterul intenționat sau neglijent al acesteia, măsurile de atenuare, gradul de cooperare și încălcările anterioare.

Procesul-verbal de constatare și sancționare și decizia de aplicare a măsurilor corective pot fi contestate la secția de contencios administrativ a tribunalului competent, **în termen de 15 zile** de la înmânare sau comunicare. Independent de sancțiunea administrativă, persoana vizată ale cărei drepturi au fost încălcate poate cere în instanță repararea prejudiciului material sau moral suferit.

4. Practica ANSPDCP în ultimele 12 luni

Sancțiunile cu valoarea cea mai ridicată au vizat insuficiența măsurilor de securitate și marketingul direct fără consimțământ. Pentru angajatori, cele mai relevante sunt însă cazurile privind datele propriilor salariați. Sancțiunile de mai jos sunt cele comunicate public de autoritate și pot face obiectul contestației în instanță.

Octombrie 2026 · Global Customer Care Services SRL · 5.000 EUR. Un atac cibernetic s-a soldat cu accesul neautorizat la datele salariaților și ale foștilor salariați. ANSPDCP a reținut încălcarea art. 32 alin. (1) lit. b) și d) și alin. (2) GDPR.

Septembrie 2026 · Tip Top Food Industry SRL · 26.236 lei (5.000 EUR). Pontajul și controlul accesului se făceau pe bază de amprentă digitală, fără temei de legalitate pentru prelucrarea datelor biometrice. ANSPDCP a reținut încălcarea art. 5 alin. (1) lit. c) raportat la art. 9 GDPR și a dispus, ca măsură corectivă, înlocuirea sistemului biometric.

August 2026 · Dormeo Home SRL · 10.517 lei (2.000 EUR). Comunicări comerciale prin SMS și apeluri. Este a doua sancțiune aplicată aceluiași operator în același an.

Iulie 2026 · Orange România SA · 523.900 lei (100.000 EUR). Prin aplicația mobilă au fost divulgate neautorizat facturile altor clienți, iar o platformă de ticketing era expusă public, fără VPN, autentificare în doi pași sau restricționare pe IP. ANSPDCP a reținut încălcarea art. 25 alin. (1) și art. 32 GDPR.

Iunie 2026 · Amato Bestseller SRL · 285.395 lei (54.361 EUR). Apeluri și comunicări comerciale automate fără consimțământul expres al destinatarilor, cu încălcarea GDPR și a Legii nr. 506/2004. Operatorul a primit patru amenzi.

Martie 2026 · Crowd Entertainment Limited · 35.000 EUR. Mesaje comerciale transmise de platforme de jocuri de noroc. Operatorul fusese sancționat și la finalul anului 2025.

Martie 2026 · ING Bank NV Amsterdam – Sucursala București · 20.388 lei (4.000 EUR). Extrasul de cont al petentei a fost eliberat unui terț, pe fondul unor măsuri de securitate inadecvate (art. 32 GDPR). Ca măsură corectivă, ANSPDCP a dispus instruirea periodică a personalului.

5. Puncte de verificare pentru angajatori

- **Evidența activităților de prelucrare.** Chiar și pentru operatorii cu sub 250 de angajați.
- **Procedura pentru încălcările de securitate.** O procedură internă de gestionare a incidentelor și de notificare a ANSPDCP în termenul de 72 de ore.
- **Securitatea platformelor interne și a celor expuse public.** Autentificare multifactor, acces restricționat și testarea periodică a eficacității măsurilor, potrivit art. 32 alin. (1) lit. d) GDPR.
- **Pontajul și accesul pe bază de date biometrice.** Este nevoie de o excepție de la art. 9 alin. (1) GDPR și de o analiză de proporționalitate care să demonstreze că mijloacele alternative nu sunt suficiente.
- **Supravegherea video și monitorizarea comunicațiilor electronice.** Condițiile art. 5 din Legea nr. 190/2018 trebuie îndeplinite cumulativ și documentate înainte de punerea în funcțiune.
- **Prelucrarea CNP în temeiul interesului legitim.** Desemnarea responsabilului cu protecția datelor și celelalte garanții ale art. 4 alin. (2) din Legea nr. 190/2018.
- **Comunicările comerciale.** Dovada consimțământului, în condițiile GDPR și ale Legii nr. 506/2004.

Concluzie

Majoritatea investigațiilor pornesc de la o singură plângere. În practică, principalul mijloc de apărare este conformitatea documentată.

Mărimea firmei nu este o apărare. Documentarea, da.

Versiunea online: https://www.frandes.law/ro/noutati/conteaza-de-fapt-marimea-firmei-gdpr-obligatiile-angajatorilor-si-practica-recen.html