SECURITATE & GDPR

Ghid GDPR pentru Website-uri

Cookie consent, politică confidențialitate, formulare, DPA și amenzi România

~22 pagini · 16 min citire · PDF A4

GDPR nu e opțional pentru niciun site care procesează date personale — inclusiv un simplu formular de contact. În România, ANSPDCP a amendat sute de firme pentru cookie-uri neconforme și lipsă politici de confidențialitate. Acest ghid îți oferă checklist-ul complet pentru conformitate fără paralizie tehnică.

Cuprins

1 Bazele GDPR — ce date procesează site-ul tău

Orice informație care identifică o persoană e dată personală: nume, email, telefon, IP, cookie ID. Dacă ai formular de contact, newsletter, Google Analytics sau Facebook Pixel — procesezi date personale. Operatorul de date (tu) e responsabil legal, indiferent că folosești furnizori terți.

Sfat ValCode
Fă un tabel simplu în Excel: Coloana 1 = tip date, Coloana 2 = sursă, Coloana 3 = scop, Coloana 4 = perioadă retenție. E baza oricărui audit GDPR.

- Date personale: orice info legată de persoană identificabilă
- Operator: firma care decide scopul procesării (tu)
- Persoană împuternicită: furnizor (hosting, email, analytics)
- Baza legală: consimțământ, contract, interes legitim, obligație legală
- Principii: transparență, minimizare, limitare scop, acuratețe
- Inventar date: listează ce colectezi, de unde, unde stochezi, cât timp

2 Banner cookie consent — implementare corectă

Cookie-urile non-esențiale (analytics, marketing) necesită consimțământ explicit înainte de activare. Banner-ul „Continuă navigarea = accepți” nu e conform GDPR. Trebuie butoane egale: Acceptă tot, Refuză tot, Personalizează — fără dark patterns.

Sfat ValCode
Folosește Cookiebot, Osano sau Klaro — soluții testate ANSPDCP. Evită plugin-uri WordPress gratuite fără audit.

- Consimțământ înainte de setare cookie non-esențial — nu după
- Buton „Refuză” la fel de vizibil ca „Acceptă”
- Granularitate: analytics separat de marketing separat de funcționale
- Dovadă consimțământ: log cu timestamp, versiune politică, alegere
- Retragere la fel de ușoară ca acordarea — link în footer
- Cookie-uri esențiale (sesiune, coș) — fără consimțământ necesar

3 Politica de confidențialitate — conținut obligatoriu

Politica de confidențialitate e contractul tău cu utilizatorul. Trebuie să explice ce date colectezi, de ce, cât timp, cui le transmiți și ce drepturi are utilizatorul. Copy-paste din template fără personalizare e la fel de riscant ca lipsa politicii.

Sfat ValCode
Actualizează politica de fiecare dată când adaugi un tool nou (chat, CRM, pixel) — data „ultima actualizare” trebuie să fie reală.

- Identitate operator: denumire, CUI, adresă, email DPO/contact
- Categorii date colectate și scopul fiecărei categorii
- Baza legală per tip de procesare
- Destinatari: hosting, email, analytics, plăți — nume furnizori
- Transferuri în afara UE: SCCs, Privacy Shield alternativ
- Perioade de retenție per categorie de date
- Drepturile utilizatorului și cum le exercită

4 Formulare web — consimțământ și minimizare

Fiecare formular colectează date — și fiecare câmp trebuie justificat. „Data nașterii” pe un formular de contact nu e minimizare. Checkbox-ul de consimțământ nu poate fi pre-bifat, iar scopul trebuie explicat în limbaj clar, nu în jargon juridic.

Sfat ValCode
Pentru formulare simple de contact, baza legală „interes legitim” (răspuns solicitare) poate înlocui consimțământul — dar documentează evaluarea.

- Câmpuri strict necesare — elimină tot ce nu e obligatoriu
- Checkbox consimțământ ne-bifat by default, cu link la politică
- Scop explicit: „Sunt de acord să fiu contactat în legătură cu...”
- Consimțământ separat pentru newsletter vs. solicitare ofertă
- CAPTCHA sau honeypot anti-spam — fără transfer date în SUA fără DPA
- Criptare transmisie: HTTPS obligatoriu, SMTP securizat

5 DPA — acorduri cu furnizorii de servicii

Orice furnizor care procesează date în numele tău (hosting, email marketing, analytics) trebuie să aibă un Data Processing Agreement semnat. Fără DPA, ești responsabil pentru nerespectarea GDPR de către furnizor. Majoritatea furnizorilor mari oferă DPA standard — trebuie doar acceptat.

Sfat ValCode
Descarcă și arhivează DPA-ul fiecărui furnizor într-un folder „GDPR/2026” — ANSPDCP poate cere dovada la control.

- DPA obligatoriu cu: hosting, email (Mailchimp, SendGrid), CRM, analytics
- Google: DPA în Google Cloud Terms, acceptă din Admin Console
- Meta: DPA în Business Tools Terms
- Furnizori RO: solicită DPA scris, chiar dacă e template
- Sub-persoane împuternicite: verifică că furnizorul are DPA cu sub-furnizori
- Revizuire anuală: la schimbare furnizor, actualizează DPA

6 Drepturile utilizatorilor — acces, ștergere, portabilitate

GDPR acordă 8 drepturi utilizatorilor, iar tu trebuie să răspunzi în 30 de zile. Cele mai frecvente solicitări: acces la date (ce aveți despre mine?) și ștergere (right to be forgotten). Procesul trebuie documentat, nu ad-hoc.

Sfat ValCode
Răspunde la cereri GDPR în max 15 zile chiar dacă legea dă 30 — arată bune-faith și reduce riscul plângerii la ANSPDCP.

- Drept de acces: export date în format structurat (JSON/CSV)
- Drept la ștergere: ștergere din DB, email, backup în 30 zile
- Drept la rectificare: corectare date incorecte la cerere
- Drept la portabilitate: transfer date către alt operator
- Drept la opoziție: oprire marketing direct imediat
- Canal cereri: email dedicat (ex: gdpr@firma.ro), nu formular generic

7 Amenzi GDPR în România — sancțiuni reale ANSPDCP

ANSPDCP (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) poate amenda până la 20 milioane € sau 4% din cifra de afaceri globală. În practică, IMM-urile primesc amenzi de 5.000–50.000 lei pentru nerespectări grave, dar repetate.

Sfat ValCode
O investiție de 500–1.500€ în conformitate GDPR e infinit mai mică decât o amendă + reputație afectată.

- Amendă maximă: 20M € sau 4% CA globală (art. 83 GDPR)
- Amenzi reale RO: 5.000–25.000 lei frecvente pentru cookie-uri
- Cauze frecvente: lipsă consimțământ, politică inexistentă, breach nenotificat
- Notificare breach: 72h la ANSPDCP dacă e risc pentru persoane
- Avertisment scris: prima abatere minoră, dacă cooperezi
- Factor agravant: date copii, date sensibile, reincidență

8 Checklist conformitate GDPR — bifează înainte de audit

Parcurge checklist-ul de mai jos și remediază golurile înainte de un control ANSPDCP sau înainte de lansare. Conformitatea GDPR e un proces continuu, nu un proiect unic — revizuiește la fiecare 6 luni sau la schimbare majoră.

Sfat ValCode
ValCode.dev integrează conformitate GDPR (cookie consent, politici, formulare) la fiecare site livrat — nu e extra, e standard.

- Inventar date personale complet și actualizat
- Banner cookie conform: consimțământ înainte, refuz egal cu accept
- Politică confidențialitate publicată, personalizată, datată
- DPA semnat cu toți furnizorii care procesează date
- Formulare: minimizare câmpuri, consimțământ explicit
- Procedură răspuns cereri GDPR documentată (30 zile)
- HTTPS pe tot site-ul, backup criptat
- Registru prelucrări (obligatoriu dacă >250 angajați sau date sensibile)

Întrebări frecvente

Am nevoie de GDPR dacă am doar un formular de contact?

Da. Orice date personale (nume, email) necesită bază legală, politică de confidențialitate și măsuri de securitate. Formularul simplu are cel mai ușor regim, dar nu e scutit.

Cât costă conformitatea GDPR pentru un site?

500–1.500€ pentru audit + implementare (banner, politici, formulare). Cookiebot costă ~10€/lună. DPA-urile cu furnizori sunt gratuite. ValCode.dev include GDPR de bază în fiecare proiect.

Implementare completă

Site + SEO + Google Ads + Mentenanță
Audit gratuit · Demo site gratuit · Răspuns în 24h

valcode.dev/contact

+40 750 205 515 · contact@valcode.dev