STABRIS

Consultanță GDPR · Audit GDPR · DPO extern

CHECKLIST DE AUTOEVALUARE A CONFORMITĂȚII GDPR

Analiză preliminară a lipsurilor · Gap Analysis

Un instrument de diagnostic rapid, destinat organizațiilor private și publice aflate la începutul procesului de conformare la Regulamentul (UE) 2016/679 (GDPR) și la Legea nr. 190/2018. În aproximativ 15 minute aflați unde se află organizația dvs. și cât de departe este de conformitate.

Ediția 2026 · Material informativ oferit gratuit de STABRIS

Cum utilizați acest checklist

Parcurgeți cele 10 secțiuni de mai jos și, pentru fiecare criteriu, bifați o singură căsuță, sincer, în funcție de situația reală din organizație:

- Da — criteriul este îndeplinit integral și puteți dovedi acest lucru cu documente. (2 puncte)
- Parțial — există ceva, dar incomplet, neactualizat sau nedocumentat. (1 punct)
- Nu — criteriul nu este îndeplinit sau nu știți dacă este. (0 puncte)

La final, adunați punctele și comparați totalul cu grila de interpretare. Scorul vă arată nivelul general de conformare — nu înlocuiește însă o evaluare detaliată a fiecărei activități de prelucrare.

> *Punctaj maxim posibil: 66 de puncte (33 criterii × 2).*

A. Guvernanța protecției datelor și responsabilizare (accountability)

Criteriu de verificare	Da	Parțial	Nu
1. Există în organizație o persoană sau un rol desemnat, cu responsabilități clare privind protecția datelor.	☐	☐	☐
2. A fost evaluată obligația de a desemna un Responsabil cu Protecția Datelor (DPO), conform art. 37 GDPR.	☐	☐	☐
3. Conducerea și angajații au beneficiat de instruire pe teme de protecția datelor în ultimele 12 luni.	☐	☐	☐
4. Există o politică internă de protecție a datelor, cunoscută și aplicată de angajați.	☐	☐	☐

B. Cartografierea datelor și temeiuri de prelucrare

Criteriu de verificare	Da	Parțial	Nu
5. Organizația deține un Registru al activităților de prelucrare (ROPA) actualizat, conform art. 30 GDPR.	☐	☐	☐
6. Pentru fiecare activitate de prelucrare este stabilit și documentat un temei legal (art. 6 GDPR).	☐	☐	☐
7. Sunt identificate categoriile speciale de date (sănătate, biometrice etc.) și regimul lor special de prelucrare.	☐	☐	☐
8. Sunt definite termene de păstrare (retenție) pentru fiecare categorie de date, după care acestea se șterg.	☐	☐	☐

C. Transparență și informarea persoanelor vizate

Criteriu de verificare	Da	Parțial	Nu
9. Site-ul organizației are o politică de confidențialitate conformă și ușor accesibilă.	☐	☐	☐
10. Există note de informare distincte pentru angajați, clienți și alți terți, adaptate fiecărui context.	☐	☐	☐
11. Notele de informare conțin toate elementele obligatorii (scop, temei, drepturi, durată, dreptul de a sesiza ANSPDCP).	☐	☐	☐

D. Drepturile persoanelor vizate

Criteriu de verificare	Da	Parțial	Nu
12. Există o procedură clară de primire și soluționare a cererilor persoanelor vizate.	☐	☐	☐
13. Puteți soluționa o cerere (acces, rectificare, ștergere, portabilitate etc.) în termenul legal de o lună.	☐	☐	☐
14. Există o evidență (registru) a cererilor primite și a modului în care au fost soluționate.	☐	☐	☐

E. Consimțământul

Criteriu de verificare	Da	Parțial	Nu
15. Acolo unde temeiul este consimțământul, acesta este obținut liber, specific și printr-o acțiune clară (nu prebifat).	☐	☐	☐
16. Păstrați dovada consimțământului: cine, când și pentru ce scop l-a acordat.	☐	☐	☐
17. Persoanele își pot retrage consimțământul la fel de ușor cum l-au acordat.	☐	☐	☐

F. Relația cu terții (persoane împuternicite și operatori asociați)

Criteriu de verificare	Da	Parțial	Nu
18. Aveți contracte de prelucrare a datelor (DPA) semnate cu toți furnizorii care prelucrează date în numele dvs. (contabilitate, IT, cloud, marketing).	☐	☐	☐
19. Contractele conțin clauzele obligatorii prevăzute de art. 28 GDPR.	☐	☐	☐
20. Obișnuiți să verificați garanțiile de securitate oferite de furnizorii care vă prelucrează datele.	☐	☐	☐

G. Securitatea datelor (măsuri tehnice și organizatorice)

Criteriu de verificare	Da	Parțial	Nu
21. Sunt implementate măsuri tehnice de securitate (control al accesului, criptare, copii de rezervă).	☐	☐	☐
22. Sunt implementate măsuri organizatorice (proceduri, angajamente de confidențialitate, instruire).	☐	☐	☐
23. Accesul la datele personale este limitat strict la persoanele care au nevoie de el pentru atribuțiile lor.	☐	☐	☐
24. Măsurile de securitate sunt documentate și revizuite periodic.	☐	☐	☐

H. Incidente și breșe de securitate

Criteriu de verificare	Da	Parțial	Nu
25. Există o procedură de identificare, gestionare și documentare a incidentelor de securitate.	☐	☐	☐

Criteriu de verificare	Da	Parțial	Nu
26. Știți cum și în ce termen (72 de ore) trebuie notificată o breșă către ANSPDCP.	☐	☐	☐
27. Există un registru al breșelor de securitate, indiferent dacă acestea au fost sau nu notificabile.	☐	☐	☐

I. Mediul online și cookie-urile

Criteriu de verificare	Da	Parțial	Nu
28. Site-ul afișează un banner de consimțământ pentru cookie-uri, cu opțiuni granulare (accept / refuz / setări).	☐	☐	☐
29. Există o politică de cookie-uri care descrie categoriile și scopurile utilizării lor.	☐	☐	☐
30. Instrumentele de marketing și de analiză (analytics, pixeli, remarketing) sunt configurate conform GDPR.	☐	☐	☐

J. Evaluări de risc (DPIA) și transferuri internaționale

Criteriu de verificare	Da	Parțial	Nu
31. A fost evaluată necesitatea unei Evaluări de Impact (DPIA) pentru prelucrările susceptibile de risc ridicat.	☐	☐	☐
32. Dacă efectuați transferuri de date în afara UE/SEE, dispuneți de garanțiile adecvate prevăzute de GDPR.	☐	☐	☐
33. Prelucrările noi sunt analizate din perspectiva protecției datelor încă din faza de proiectare (privacy by design).	☐	☐	☐

Interpretarea scorului

Adunați punctele obținute (Da = 2, Parțial = 1, Nu = 0) și identificați banda în care vă încadrați:

Punctaj	Nivel	Ce înseamnă
Peste 80% din punctaj	**Nivel avansat**	Aveți o bază solidă. Atenție însă: conformitatea GDPR nu este un proiect încheiat, ci un proces continuu. Chiar și la acest nivel, un audit independent identifică aproape întotdeauna lipsuri pe care autoevaluarea nu le surprinde.
50% – 80%	**Nivel intermediar**	Există fundament, dar și lipsuri semnificative care expun organizația la riscuri și la posibile sancțiuni. Sunt necesare prioritizare și remediere structurată.
25% – 49%	**Nivel incipient**	Lipsuri majore în mai multe zone-cheie. Organizația se află la început de drum și are un risc ridicat în cazul unei sesizări sau al unui control ANSPDCP.
Sub 25%	**Neconform**	Elementele de bază lipsesc. Este necesară o intervenție urgentă și coordonată pentru a aduce organizația în parametri de conformitate.

Ce urmează?

Acest checklist vă arată unde aveți lipsuri — dar nu și cum se acoperă fiecare dintre ele. Aici intervine STABRIS. Traducem rezultatul autoevaluării într-un plan concret de conformare, adaptat activității dvs.:

- Audit GDPR — o evaluare independentă și detaliată a tuturor activităților de prelucrare, cu raport de neconformități și plan de măsuri.
- Implementare GDPR — elaborarea și punerea în aplicare a registrelor, politicilor, procedurilor și contractelor adaptate organizației dvs.
- DPO extern — preluarea funcției de Responsabil cu Protecția Datelor și menținerea conformității în timp.

Solicitați o evaluare gratuită a rezultatului dvs.

Website: [www.stabris.ro] **Email:** [contact@stabris.ro] **Telefon:** [0332.402.192]