

Enterprise Questionnaire Privacy Security

Sursă: 12-enterprise-questionnaire-privacy-security.md

Generat: 2026-02-25

QUESTIONNAIRE ENTERPRISE

Privacy + Security (Vendor Due Diligence)

Document: Set întrebări clarificare vendor

Versiune: 1.0

Actualizat: 25 februarie 2026

Scop: Suport pentru revizuire procurement, juridic și IT security.

1. Model juridic și roluri

1. Cum este delimitat contractual fluxul în care clientul este Operator și vendorul este Processor?
2. Ce prelucrări rămân în responsabilitatea vendorului ca Operator (website/admin) și ce prelucrări intră sub DPA?
3. Ce instrucțiuni standard ale Operatorului sunt implementate by default la onboarding?

2. Localizare, monitorizare și proportionalitate

4. Ce date de localizare se colectează exact (coordonate, geofence status, timestamp) și în ce momente?
5. Cum este prevenită colectarea în afara programului (schedule guard, blocare, mark for review)?
6. Ce alternativă operațională există când localizarea nu este proporțională (pontaj manual / fallback)?
7. Ce template-uri sunt oferite pentru informarea angajaților și pentru evaluarea DPIA/LIA?

3. Retenție, ștergere și lifecycle

8. Care sunt retențiile numerice pe categorii (pontaj, snapshots, audit logs, DSAR, facturare)?
9. Ce joburi automate de ștergere rulează și cum se dovedește execuția lor în audit?
10. Care este fluxul de export, returnare și ștergere la încetarea contractului?

4. Subprocesatori și transferuri internaționale

11. Care sunt subprocesatorii care pot primi date de angajați și în ce jurisdicții operează?
12. Ce mecanisme sunt aplicate pentru transferurile extra-SEE (SCC/TIA/alte garanții)?
13. Ce procedură contractuală de notificare/opoziție există la schimbarea subprocesatorilor?

5. Securitate și incident response

14. Ce controale de securitate admin sunt active (RBAC, MFA, audit trail, segregare tenant)?

15. Care este SLA-ul de notificare incident către Operator și care este conținutul minim al notificării?

16. Ce evidențe tehnice suplimentare pot fi furnizate pe NDA pentru audit IT security?

6. Cookie-uri, tracking și marketing

17. Care cookies/trackere sunt strict necesare vs. opționale și ce durate au?

18. Cum se documentează consimțământul și cum este implementată retragerea acestuia?

19. Ce furnizori terți de analytics/marketing primesc date și în ce condiții?

7. AI și analitice avansate

20. Ce funcții AI sunt active pentru tenantul clientului și ce date sunt procesate?

21. Cum este controlată contractual utilizarea funcțiilor AI pentru a respecta instrucțiunile Operatorului?

8. Decizie de go-live

22. Ce gap-uri rămase au termen/owner de remediere înainte de go-live?

23. Ce controale trebuie validate în UAT pentru semnare finală (off-hours, retenție, DSAR, export)?

Notă de utilizare

Acest questionnaire este destinat etapei de clarificare enterprise. Nu înlocuiește analiza juridică independentă a Operatorului și nu substituie clauzele contractuale finale.