Raport Audit GDPR 2026 02 25

Sursă: 09-raport-audit-gdpr-2026-02-25.md Generat: 2026-02-25

RAPORT DE AUDIT GDPR

ConstructorPRO / PontajAutomat (context client: ACOMIN SA)

Data auditului: 25 februarie 2026

Tip audit: tehnico-juridic intern (code + documente + fluxuri operaționale)

Obiect: determinarea gradului de conformitate GDPR/ePrivacy și capacitatea de demonstrare a conformității (principiul responsabilității).

---

1) Limită juridică și metodologică

Acest document reprezintă o evaluare tehnico-juridică internă, nu opinie juridică externă emisă de avocat și nu substituie un control al autorității de supraveghere (ANSPDCP).

Auditul a fost realizat pe:

- cod backend/frontend/mobile (Convex + React + React Native);
- documentația contractuală și de privacy din legal/;
- politicile interne din docs/_reference/legal.

---

2) Cadru normativ aplicabil (verificat la 25.02.2026)

1. Regulamentul (UE) 2016/679 (GDPR), inclusiv art. 5, 6, 7, 12, 15, 17, 24, 25, 30, 32, 35, 44-46.

2. Legea nr. 190/2018 (măsuri de punere în aplicare GDPR în România), inclusiv art. 5 privind monitorizarea la locul de muncă.

3. Legea nr. 506/2004 (comunicații electronice), art. 4 alin. (5) pentru stocarea/accesul informației pe terminal (cookie/trackere) pe baza consimțământului informat, cu excepții strict necesare.

4. Legea nr. 53/2003 - Codul muncii, art. 119 (obligația angajatorului de evidență a orelor de muncă).

5. Contractele și anexele interne aplicabile: MSA, DPA, Privacy Policy/Cookies, Security/TOMs/Retenții.

Surse oficiale:

- GDPR (EUR-Lex): https://eur-lex.europa.eu/eli/reg/2016/679/oj
- Directiva ePrivacy 2002/58/CE (EUR-Lex): https://eur-lex.europa.eu/eli/dir/2002/58/2009-12-19
- Legea 190/2018 (Portal Legislativ): https://legislatie.just.ro/Public/DetaliiDocument/203151
- Legea 506/2004 (Portal Legislativ): https://legislatie.just.ro/Public/DetaliiDocumentAfis/56973

- **Codul muncii (Portal Legislativ): https://legislatie.just.ro/Public/DetaliiDocument/282881**

---

3) Concluzie executivă (verdict)

Verdict: la data auditului, platforma este în stare de conformitate parțială, cu neconformități critice și majore.

În această stare, nu se poate susține juridic conformitatea GDPR deplină și există risc material de constatare negativă la control (în special pe ePrivacy/cookies, exercitarea drepturilor și coerența retenției).

---

4) Matrice sintetică de conformitate

- Domeniu | Temei legal | Status | Concluzie
- Principii GDPR (legalitate, transparență, minimizare, stocare) | Art. 5 GDPR | Parțial | Inconsistențe de retenție și logare PII
- Temeiuri de prelucrare / consimțământ | Art. 6-7 GDPR | Parțial | full_auto mobile poate ocoli consimțământul explicit
- Informare și facilitarea drepturilor | Art. 12 GDPR | Neconform | UI web afișează drepturi fără executare reală completă
- Drept acces/portabilitate | Art. 15 GDPR | Neconform (web) / Parțial (API) | Buton export fără handler în web
- Drept ștergere | Art. 17 GDPR | Parțial | Erasure incomplet (disputes), fluxuri de cereri fragmentate
- Privacy by design/default | Art. 25 GDPR | Neconform | identitySnapshot în clar în legal hold
- Securitate prelucrare | Art. 32 GDPR | Parțial | Loguri cu payload PII în webhook-uri
- Registrul prelucrărilor / accountability | Art. 30 + art. 5(2) GDPR | Parțial | Nu există în repo dovadă formală ROPA semnată
- DPIA monitorizare sistematică | Art. 35 GDPR + Legea 190/2018 | Parțial / Neconform formal | Necesitatea DPIA este recunoscută, dar lipsește dosarul formal complet
- Subprocesatori și transfer SEE/non-SEE | Art. 28 + 44-46 GDPR | Parțial | date nefinalizate în DPA (ex. BulkGate/SMS Advert)
- Cookies/trackere non-esențiale | Legea 506/2004 art. 4(5) | Neconform | Clarity este injectat înainte de consimțământ
- Evidență timp de muncă | Codul muncii art. 119 | Conform (funcțional) | există funcționalitate de pontaj, dar trebuie armonizată retenția

---

5) Constatări detaliate (cu severitate)

F-01 (CRITIC) - Dreptul la portabilitate neexecutabil în web UI

- Temei legal: art. 12 și art. 15 GDPR.
- Constatare: butonul „Exportă Datele Mele” este doar vizual, fără onClick.
- Evidență:
- apps/demo/pages/Privacy.tsx:519
- apps/demo/pages/Privacy.tsx:542-545
- Risc: persoana vizată nu poate exercita dreptul în interfața declarată.

F-02 (CRITIC) - Tracking non-esențial înainte de consimțământ (Clarity)

- Temei legal: Legea 506/2004 art. 4 alin. (5), art. 6 GDPR.
- Constatare: script Microsoft Clarity este injectat direct în index.html, independent de starea de consimțământ.
- Evidență:
- apps/demo/index.html:60-67
- comparativ: GA/Meta încărcate doar cu consimțământ în apps/demo/hooks/useCookieConsent.ts:177-186
- Risc: expunere directă pe ePrivacy/cookies.

F-03 (MAJOR) - Export GDPR backend fără control complet de autorizare în action

- Temei legal: art. 5(1)(f), art. 15 GDPR.
- Constatare: exportWorkerData este action, iar comentariul intern spune că autorizarea trebuie făcută de caller; controlul nu este închis în același endpoint.
- Evidență: apps/demo/convex/gdpr.ts:23-45
- Risc: acces neautorizat/cross-tenant dacă e apelat direct sau prin wrapper incomplet.

F-04 (MAJOR) - Erasure incomplet: disputele nu sunt anonimizate

- Temei legal: art. 17 GDPR.
- Constatare: în processErasure, pasul de disputes este comentat, disputesCount = 0.
- Evidență: apps/demo/convex/gdpr.ts:308-312
- Risc: ștergere incompletă a datelor personale.

F-05 (MAJOR) - Legal hold cu identitate în clar (identitySnapshot)

- Temei legal: art. 5(1)(f), art. 25, art. 32 GDPR.
- Constatare: snapshot-ul identității este stocat JSON.stringify(...) fără criptare.
- Evidență:
- apps/demo/convex/gdpr.ts:263-271
- apps/demo/convex/schema.ts:3941
- Risc: menținere PII în clar după inițierea ștergerii.

F-06 (MAJOR) - Bypass de consimțământ în modul mobil full_auto

- Temei legal: art. 6-7 GDPR, art. 5 Legea 190/2018 (proporționalitate/garanții).
- Constatare: forceEnable() omite verificarea consimțământului și este apelat automat la mappedMode === 'full_auto'.
- Evidență:
- apps/mobile/src/services/seamlessTimeTracking.ts:1543-1559
- apps/mobile/src/hooks/useSeamlessTracking.ts:542-545
- Risc: nealiniere între baza legală declarată și comportamentul efectiv.

F-07 (MAJOR) - Inconsistență materială de retenție (30 zile vs 365 zile vs 3 ani)

- Temei legal: art. 5(1)(a) și 5(1)(e) GDPR.
- Constatare: valori de retenție diferite în cod, UI și documente.
- Evidență:

- **cleanup 30 zile: apps/demo/convex/scheduledJobs.ts:1151-1152, 1219-1220**
- audit privacy 365 zile: apps/demo/convex/secureTimeEntries.ts:1062
- default mobil 365 zile: apps/mobile/src/services/dataPolicy.ts:75
- UI web 3 ani locație: apps/demo/pages/Privacy.tsx:493
- policy internă 3 ani/30 zile: docs/_reference/legal/GDPR_DATA_COLLECTION_POLICY.md:393-397
- document legal 30 zile snapshots: legal/06-SECURITY-TOMS-RETENTII.md:160
- Risc: transparență deficitară, imposibilitate de justificare unitară la control.

F-08 (MAJOR) - Fluxuri paralele de cereri de ștergere, fără orchestrare unică

- Temei legal: art. 12 și 17 GDPR.
- Constatare: coexistă gdprRequests și dataDeletionRequests, fără procesor comun identificat pentru al doilea.
- Evidență:
- apps/demo/convex/schema.ts:3908-3932 (gdprRequests)
- apps/demo/convex/schema.ts:4720-4731 (dataDeletionRequests)
- inserare doar în: apps/demo/convex/secureTimeEntries.ts:1400
- utilizări suplimentare absente: căutare dataDeletionRequests doar în cele 2 fișiere de mai sus
- Risc: cereri nerezolvate, risc depășire termen legal.

F-09 (MAJOR) - Loguri cu PII (nume/payload lead)

- Temei legal: art. 5(1)(c), 5(1)(f), art. 32 GDPR.
- Constatare: se loghează nume worker și payload-uri webhook brute (pot include telefon/email).
- Evidență:
- apps/demo/convex/secureTimeEntries.ts:690, 706
- apps/demo/convex/http.ts:346, 547
- Risc: supraexpunere în infrastructura de loguri.

F-10 (MEDIU) - Nealinieri în dosarul subprocesatori/transferuri

- Temei legal: art. 28 și 44-46 GDPR.
- Constatare: în DPA apar elemente „de confirmat” pentru SMS provider; documentele nu sunt perfect aliniate.
- Evidență:
- legal/03-DPA-GDPR.md:109
- legal/07-PRIVACY-COOKIES.md:124
- Risc: lacună de accountability contractuală.

F-11 (MEDIU) - DPIA recunoscută ca obligatorie, dar lipsă dosar formal finalizat

- Temei legal: art. 35 GDPR + Legea 190/2018.
- Constatare: policy-ul recunoaște explicit obligativitatea, fără document formal de DPIA completat/semnat identificat în repo.
- Evidență: docs/_reference/legal/GDPR_DATA_COLLECTION_POLICY.md:476-486
- Risc: neconformitate formală la cerere de probă.

---

6) Măsuri obligatorii de remediere (plan 30/60/90 zile)

În 0-30 zile (blocante pentru conformitate declarată)

1. Implementare onClick real pentru export și ștergere în web (Privacy.tsx) + confirmare traseu backend.
2. Oprire Clarity până la gating explicit pe consimțământ (sau încărcare condiționată strict după opt-in).
3. Introducere verificare autorizare direct în gdpr.exportWorkerData.
4. Remediere processErasure pentru disputes.
5. Eliminare loguri PII/payload brut; introducere redaction middleware.
6. Unificare retenție într-o sursă unică de adevăr (cod + legal + UI).

În 31-60 zile

1. Criptare/pseudonimizare gdprLegalHolds.identitySnapshot.
2. Unificare flux DSAR (gdprRequests vs dataDeletionRequests) cu SLA și audit trail unic.
3. Finalizare anexa subprocesatori (DPA-uri, locații, SCC/TIA evidențiate).

În 61-90 zile

1. DPIA formal complet + aprobare management/DPO.
2. ROPA (Registrul activităților) formal și actualizat.
3. Test de conformitate periodic (quarterly) cu checklist legal + technical controls.

---

7) Proba de conformitate necesară după remediere

Pentru a susține „conform GDPR” într-un audit extern, dosarul minim trebuie să includă:

1. versiuni finale ale politicilor (retenție, privacy, cookies) perfect aliniate cu codul;
2. DPIA semnată + măsuri implementate;
3. ROPA actualizat;
4. contracte DPA + SCC + TIA pentru fiecare subprocesator relevant;
5. evidențe DSAR (cereri, timpi de răspuns, rezultate);
6. evidențe tehnice (capturi/loguri redacted) privind consimțământul și retenția.

---

8) Concluzie juridică finală

La data de 25 februarie 2026, pe baza probelor tehnice și documentare analizate, nu se poate certifica conformitatea GDPR deplină pentru platformă în forma curentă.

Poziția juridică prudentă este: conformitate parțială, cu neconformități critice/majore remediabile.

După implementarea măsurilor din secțiunea 6 și completarea dosarului de accountability (DPIA/ROPA/DPA complete), platforma poate fi poziționată defensabil ca „GDPR-ready”.