Security Toms Retentii

Sursă: 07-security-toms-retentii.md Generat: 2026-02-25

MĂSURI TEHNICE ȘI ORGANIZATORICE (TOMs)

!Pontaj Automat (https://pontajautomat.ro/logo.png)

PONTAJ AUTOMAT

by ConstructorPro

Document: Anexa Securitate și Retenții

Versiune: 2.0

Clasificare: Confidențial - Uz Intern și Clienți

Data: Ianuarie 2026

- Câmp | Valoare
- Furnizor | ADAPT INDUSTRIES SRL
- CUI | 40595773
- Reg. Com. | J33/428/2019
- Sediu | Str. Slavici Ion 2, Câmpulung Moldovenesc, Suceava, 725100
- DPO | dpo@pontajautomat.ro
- Securitate | security@pontajautomat.ro

SECȚIUNEA A
MĂSURI TEHNICE ȘI ORGANIZATORICE

Prezenta anexă descrie măsurile implementate de Furnizor în conformitate cu Art. 32 GDPR pentru asigurarea unui nivel de securitate adecvat riscurilor.

A.1. CONTROLUL ACCESULUI ȘI AUTENTIFICAREA

- Măsură | Implementare

- **Autentificare | Serviciu specializat (Clerk) cu suport MFA**
- Controlul accesului | Role-Based Access Control (RBAC)
- Principiul minimului privilegiu | Fiecare rol are doar permisiunile necesare
- Roluri disponibile | Administrator, Manager, Șef Șantier, Maistru, Contabil, Muncitor, Client
- Recomandare | 2FA obligatoriu pentru rolurile administrative

---

A.2. IZOLAREA MULTI-TENANT

- Măsură | Implementare
- Separare date | Fiecare înregistrare include companyId
- Interogări | Filtrate automat pe baza companiei autentificate
- Indexare | Index by_company pe toate tabelele de date
- Prevenție cross-tenant | Validare la nivel de middleware pentru fiecare operațiune

---

A.3. CRIPTARE ȘI PROTECȚIA DATELOR

- Aspect | Măsură
- Date în tranzit | TLS 1.2+ pentru toate conexiunile
- Date în repaus | Criptare la nivelul furnizorului de cloud
- Secrete și chei | Management conform bunelor practici (variabile de mediu securizate)
- Parole | Hash-uri bcrypt, fără stocare în clar

A.4. JURNALIZARE ȘI AUDIT TRAIL

Sistemul menține jurnale de audit pentru:

- Crearea, modificarea și ștergerea entităților
- Aprobările de pontaj
- Exporturile de date
- Modificările de configurație
- Tentativele de autentificare

Fiecare înregistrare include: timestamp, userId, companyId, acțiune, entitate.

A.5. BACKUP ȘI RECUPERARE

- Parametru | Valoare
- Frecvență backup | Zilnic (conform politicile furnizorului Convex)
- Retenție backup | Conform SLA-ului furnizorului de infrastructură
- Proceduri restaurare | Best effort, cu prioritizare conform severității
- Testare | Periodic, conform procedurilor interne

A.6. SECURITATEA SUPORTULUI TEHNIC

- Măsură | Descriere
- Acces la date | Exclusiv pe baza tichetelor de suport
- Personal autorizat | Doar angajații desemnați pentru suport
- Jurnalizare | Log al tuturor accesărilor administrative
- Confidențialitate | Obligații contractuale pentru tot personalul

---

A.7. MINIMIZAREA DATELOR

- Practică | Implementare
- Snapshots activitate | Ștergere automată după 30 zile
- Agregări | Preferință pentru workerDailyAnalytics vs. date brute
- Colectare | Doar în sesiunea de lucru (între check-in și check-out)
- Export | Posibilitate de anonimizare la cerere

A.8. PROCEDURĂ INCIDENT RESPONSE

Procesul de răspuns la incidente urmează 4 faze:

-
- DETECTARE ▶ CONȚINERE ▶ REMEDIERE ▶ NOTIFICARE
- & TRIERE & IZOLARE & RECUPERARE & RAPORTARE
-

Faza 1 - Detectare și Triere:

- Înregistrarea incidentului în sistemul intern
- Clasificare: securitate / disponibilitate / date personale
- Evaluarea severității și impactului

Faza 2 - Conținere și Izolare:

- Izolarea sistemelor afectate
- Revocare tokenuri și sesiuni compromise
- Prevenirea extinderii incidentului

Faza 3 - Remediere și Recuperare:

- Aplicarea patch-urilor necesare
- Rotația cheilor și credențialelor
- Restaurare din backup dacă este necesar

Faza 4 - Notificare și Raportare:

- Notificarea Clientului fără întârzieri nejustificate
- Furnizarea informațiilor: natură, date afectate, măsuri

- **Cooperare pentru obligațiile legale ale Operatorului**

SECȚIUNEA B
POLITICA DE RETENȚIE

Perioadele de retenție sunt stabilite conform cerințelor legale și principiului minimizării datelor:

- Categorie | Retenție | Bază legală / Justificare | Observații
- workerActivitySnapshots | 30 zile | Minimizare date | Ștergere automată (cron 03:00 UTC)
- timeEntries (pontaj) | 10 ani | Art. 119 Codul Muncii, Legea contabilității | Evidențe obligatorii
- workerDailyAnalytics | 24 luni | Analiză operațională | Recomandare; configurabil
- auditLog / activityLogs | 24 luni | Securitate și trasabilitate | Extensibil pentru Enterprise
- absences (inclusiv CM) | 10 ani | Legislația muncii | Acces restricționat; date sensibile
- workerContracts | 10 ani | Legislația muncii | Arhivare contractuală
- dailyLogs + fotografii | 24 luni | Documentare proiecte | Sau final proiect + 12 luni
- REGES submit status | 5 ani | Dovadă operațională | Pentru audit și remedieri
- Date facturare | 10 ani | Legea contabilității | Obligație legală

Notă importantă:

- Clientul (Operatorul) este responsabil să adopte politici de retenție proporționale cu scopurile prelucrării
- Perioadele pot fi ajustate prin Comandă, cu asumarea responsabilității de către Client
- La cerere, Clientul poate solicita ștergere anticipată, cu excepția datelor cu obligație legală de păstrare

---

SECȚIUNEA C
PROCEDURA DE NOTIFICARE BREACH

În conformitate cu Art. 33-34 GDPR:

C.1. Obligațiile Furnizorului (Processor)

- Obligație | Termen
- Notificare către Client | Fără întârzieri nejustificate după constatare
- Conținut notificare | Natura, date afectate, perioada, măsuri luate, recomandări
- Cooperare | Furnizare informații pentru notificarea autorităților/persoanelor vizate

C.2. Obligațiile Clientului (Operator)

- Obligație | Termen
- Evaluare incident | Imediat după primirea notificării
- Notificare ANSPDCP | Maximum 72 ore de la constatare (dacă este cazul)
- Informare persoane vizate | Fără întârzieri nejustificate (dacă riscul este ridicat)

SECȚIUNEA D

PACHETUL ANGAJATORULUI

D.1. DECLARAȚIE OPERATOR (de semnat de reprezentantul Clientului)

-
- DECLARAȚIE DE CONFORMITATE OPERATOR
- (GDPR Art. 24, 26, 28)
-
- Subsemnatul(a) _____,
- în calitate de reprezentant legal al _____,
- CUI _____, în calitate de Operator de date cu caracter personal,
- DECLAR PE PROPRIA RĂSPUNDERE CĂ:
- 1. Am stabilit un temei legal valid pentru prelucrarea datelor cu caracter
- personal ale angajaților/colaboratorilor prin intermediul Platformei
- Pontaj Automat, în conformitate cu Art. 6 GDPR.
- 2. Am evaluat necesitatea și proporționalitatea prelucrării datelor de
- locație și activitate în raport cu scopurile urmărite.
- 3. Am informat sau voi informa toate persoanele vizate ÎNAINTE de
- activarea funcționalităților de monitorizare, în conformitate cu
- Art. 13-14 GDPR, punând la dispoziție nota de informare anexată.
- 4. Colectarea datelor de locație și activitate este limitată exclusiv
- la sesiunile de lucru și servește scopuri legitime de organizare
- și evidență a muncii.
- 5. Am definit și documentat perioadele de retenție pentru fiecare
- categorie de date și pot justifica aceste perioade.
- 6. NU voi utiliza Platforma pentru:
- - Supraveghere ilegală sau disproporționată
- - Monitorizare în afara raporturilor de muncă
- - Hărțuire, discriminare sau represalii
- 7. Orice decizie cu impact asupra angajaților (inclusiv decizii
- disciplinare) va fi luată cu revizuire umană, nu exclusiv pe
- baza rezultatelor automatizate ale Platformei.
- 8. Am implementat sau voi implementa măsuri organizatorice interne
- pentru protecția datelor, inclusiv politici de acces și formare.
- Nume/Funcție: _____
- Semnătura: _____
- Data: ___ / ___ / 202___

- **Ștampila societății: _____**
-

D.2. CHECKLIST EVALUARE IMPACT (DPIA)

Pentru activarea funcționalităților de locație în fundal și/sau monitorizare activitate, se recomandă evaluarea următoarelor aspecte:

- Nr. | Element | Verificat
- 1 | Descrierea detaliată a prelucrării (ce date, când, cum, cine accesează) |
- 2 | Scopurile prelucrării și interesul legitim urmărit |
- 3 | Evaluarea necesității și proporționalității |
- 4 | Identificarea riscurilor pentru persoanele vizate |
- 5 | Măsuri de atenuare a riscurilor (limitare temporală, roluri, retenție scurtă) |
- 6 | Transparență și informare (nota de informare disponibilă) |
- 7 | Mecanism pentru exercitarea drepturilor |
- 8 | Concluzia evaluării și aprobare internă |

Recomandare: Documentați evaluarea și păstrați-o pentru audit.

D.3. NOTĂ DE INFORMARE ANGAJAȚI (Template)

Acest template trebuie personalizat de Client și furnizat angajaților înainte de activarea monitorizării.

-
- NOTĂ DE INFORMARE PRIVIND PRELUCRAREA DATELOR
- CU CARACTER PERSONAL
- (GDPR Art. 13 - Art. 14)
-
- OPERATOR (Angajator):
- Denumire: _____
- CUI: _____
- Sediu: _____
- Contact DPO/HR: _____
- PERSOANĂ ÎMPUTERNICITĂ (Platformă):
- ADAPT INDUSTRIES SRL, CUI 40595773
- DPO: dpo@pontajautomat.ro
-
- CE DATE COLECTĂM
-
- • Identificare: nume, prenume, număr de telefon, adresă email, funcție

- • **Pontaj: ore de check-in și check-out, pauze înregistrate**
- • Locație: coordonate GPS, acuratețe, încadrare în zone de lucru
- (DOAR în timpul programului de lucru)
- • Activitate: detectare mișcare, pași (dacă funcția este activată)
- • Tehnice: identificator dispozitiv, versiune aplicație
-
- CÂND COLECTĂM
-
- • EXCLUSIV în timpul sesiunii de lucru (între check-in și check-out)
- • Conform programului de lucru și setărilor stabilite de angajator
- • Colectarea ÎNCETEAZĂ automat la check-out
-
- DE CE COLECTĂM
-
- • Evidența timpului de muncă conform Art. 119 Codul Muncii
- • Organizarea operațională a activității pe șantiere/proiecte
- • Verificarea prezenței în locațiile de lucru desemnate
- • Generarea rapoartelor de activitate
- • Prevenirea fraudei și asigurarea securității
-
- TRANSFERURI ȘI DESTINATARI
-
- Datele pot fi accesate de:
- • Personalul autorizat al angajatorului (manageri, HR, contabilitate)
- • Furnizorul platformei (ADAPT INDUSTRIES SRL) - în calitate de Processor
- • Subprocesatori tehnici (hosting, autentificare) - unii în afara SEE,
- cu garanții SCC
-
- PERIOADE DE PĂSTRARE
-
- • Snapshots locație/activitate: 30 zile
- • Pontaj (ore lucrate): 10 ani (obligație legală)
- • Jurnale de audit: 24 luni
- • Restul: conform politicii angajatorului
-
- DREPTURILE TALE
-

- **Ai dreptul de a solicita:**
- ✓ ACCES la datele tale personale
- ✓ RECTIFICAREA datelor incorecte
- ✓ ȘTERGEREA datelor (în limitele obligațiilor legale)
- ✓ RESTRICȚIONAREA prelucrării
- ✓ OPOZIȚIA la prelucrare în anumite cazuri
- ✓ PORTABILITATEA datelor într-un format structurat
- Pentru exercitarea drepturilor, contactează: [email HR/DPO angajator]
- Ai dreptul de a depune PLÂNGERE la ANSPDCP (www.dataprotection.ro).
-
- DECIZII AUTOMATIZATE
-
- Platforma NU ia decizii automatizate cu efecte juridice.
- Scorurile și analizele generate sunt DOAR INFORMATIVE.
- Orice decizie care te afectează va fi luată cu revizuire umană.
-
- Am luat la cunoștință prezenta notă de informare:
- Semnătură angajator: _____ Semnătură salariat: _____
- Data: ___ / ___ / 202___ Data: ___ / ___ / 202___
-

PONTAJ AUTOMAT by ConstructorPro

ADAPT INDUSTRIES SRL | CUI 40595773 | J33/428/2019

Str. Slavici Ion 2, Câmpulung Moldovenesc, Suceava, 725100

0746 844 7XX | security@pontajautomat.ro

www.pontajautomat.ro

Document confidențial. Versiune 2.0 | Ianuarie 2026