GDPR for Software Engineers & Architects

Ghid practic de conformitate tehnică: De la concepte juridice la Arhitectură, Baze de Date și Cod

Modulul 1: Concepte fundamentale traduse în limba tehnică

GDPR (Regulamentul General privind Protecția Datelor - UE 2016/679) nu este doar un document legal, ci un set de cerințe funcționale și non-funcționale care afectează direct arhitectura software-ului, structura bazelor de date și logica de business.

1.1. Ce reprezintă Datele cu Caracter Personal (PII)?

Multe echipe de dezvoltare consideră eronat că datele personale se limitează la Nume, CNP sau Email. În arhitectura software, **PII (Personally Identifiable Information)** reprezintă orice dată care permite identificarea directă sau indirectă a unui utilizator:

- **Date de identificare directă:** Nume, prenume, adresa de email, număr de telefon, adresa poștală.
- **Identificatori tehnici:** Adresă IP (statică sau dinamică), User ID / GUID, Cookie ID-uri, MAC address, token-uri de sesiune, ID-uri de dispozitiv (IDFA/GAID).
- **Date privind locația:** Coordonate GPS, date despre celula GSM, IP-geolocation precis.
- **Categorii speciale de date (Art. 9 GDPR):** Date biometrice, date despre sănătate, orientare politică/religioasă, origini etnice. Acestea necesită criptare strictă și mecanisme speciale de consimțământ.

1.2. Rolurile din ecosistemul de date

Rol GDPR	Echivalent în Dezvoltare Software	Responsabilitate Tehnică
Data Controller (Operator)	Clientul sau compania care deține aplicația / afacerea.	Definește de ce și ce date se colectează (Business Requirements).

Rol GDPR	Echivalent în Dezvoltare Software	Responsabilitate Tehnică
Data Processor (Persoană împuternicită)	Furnizorul SaaS, agenția de software dev, sau providerul de Cloud (AWS, Azure, GCP).	Procesează datele strict conform instrucțiunilor Controller-ului și implementează măsurile de securitate.
Data Subject (Persoană vizată)	Utilizatorul final al aplicației (End User).	Beneficiarul drepturilor (Export, Ștergere, Rectificare).

Modulul 2: Principii de Design – Privacy by Design & Privacy by Default

Articolul 25 GDPR impune ca protecția datelor să fie integrată din faza de proiectare/arhitectură (*Privacy by Design*) și configurată la nivelul cel mai restrictiv în mod implicit (*Privacy by Default*).

2.1. Minimimizarea datelor (Data Minimization)

Nu colectați și nu stocați date de care aplicația nu are nevoie directă pentru funcționare. Fiecare câmp suplimentar adăugat în bază de date reprezintă un risc de securitate și o obligație legală.

```
// NERECOMANDAT (Anti-pattern): Colectare excesivă la înregistrare
POST /api/register
{
  "email": "user@example.com",
  "password": "hashed_password",
  "full_name": "Ion Popescu",
  "birth_date": "1990-05-15", // Neesențial dacă aplicația nu e restricted by age
  "gender": "M",              // Neesențial
  "ip_address": "192.168.1.1"
}

// RECOMANDAT (Best Practice): Minimimizarea datelor
POST /api/register
{
```

```
  "email": "user@example.com",
  "password": "hashed_password"
}
```

2.2. Limitarea stocării (Storage Limitation)

Fiecare tabel care conține PII trebuie să aibă o politică clară de retenție (Retention Policy). Implementați job-uri automate de curățare (CRON / background workers) sau mecanisme de TTL (Time-To-Live) la nivel de bază de date.

Modulul 3: Arhitectura Sistemului pentru Drepturile Utilizatorilor

GDPR oferă utilizatorilor drepturi speciale care trebuie traduse în functionalități de backend și frontend.

3.1. Dreptul de a fi uitat / Ștergerea Datelor (Art. 17 GDPR)

Când un utilizator solicită ștergerea contului, aplicația trebuie să elimine PII din toate mediile (Baze de date, Caching, Loguri, Servicii terțe, Backup-uri).

Strategii tehnice de implementare:

- **Hard Delete (Ștergere fizică):** Ștergerea definitivă a randului din baza de date. Poate strica integritatea referențială dacă aveți chei străine legate de tranzacții financiare.
- **Anonimizare (Pseudonimizare ireversibilă):** Recomandată pentru păstrarea integrității datelor analitice sau financiare.

```
-- În loc să ștergem comanda/factura, anonomizăm datele de identificare:
UPDATE users
SET
  email = CONCAT('deleted_', id, '@anonymized.local'),
  first_name = 'ANONYMIZED',
  last_name = 'ANONYMIZED',
  phone = NULL,
  is_deleted = TRUE,
  deleted_at = NOW()
WHERE id = 1042;
```

3.2. Dreptul la Portabilitatea Datelor (Art. 20 GDPR)

Aplicația trebuie să ofere un endpoint automatizat prin care utilizatorul își poate descărca toate datele într-un format structurat, utilizat în mod curent și citibil prin cale automată (JSON, CSV, XML).

```
GET /api/v1/user/export-data
Response: 200 OK (Content-Type: application/json)
{
  "profile": { "id": 1042, "email": "user@domain.com", "created_at": "2024-01-10" },
  "orders": [ ... ],
  "activity_logs": [ ... ]
}
```

Modulul 4: Managementul Logurilor și Stocarea Datelor

4.1. Igiena logurilor de aplicație

Risc major: Inserarea PII sau a datelor sensibile în fisierele de loguri (ex: ELK Stack, Datadog, Papertrail, fișiere locale .log).

- **Ce NU se loghează NICIODATĂ:** Parole în text clar, token-uri de acces (JWT), date de card (PAN/CVV), CNP-uri.
- **Mascarea PII în loguri:** Folosiți middleware sau interceptoare pentru sanitizarea payload-urilor înainte de scriere.

```
// Exemplu de Sanitizer Middleware în Node.js / Express
function sanitizeLogData(data) {
  const sensitiveKeys = ['password', 'token', 'credit_card', 'email'];
  const sanitized = { ...data };

  for (let key in sanitized) {
    if (sensitiveKeys.includes(key.toLowerCase())) {
      sanitized[key] = '***REDACTED***';
    }
  }
  return sanitized;
}
```

4.2. Criptarea datelor (In-Transit & At-Rest)

- **In-Transit:** TLS 1.2+ obligatoriu pe toate rutele (HTTPS, WSS, conexiuni DB).
- **At-Rest:** Criptarea coloanelor sensibile (ex: AES-256) în baza de date și criptarea volumelor de stocare (AWS EBS encryption, LUKS).

Modulul 5: Consimțământul și Integrările cu Terții (Third-Party Services)

5.1. Gestionarea Consent-ului în Baza de Date

Consimțământul pentru scopuri opționale (Marketing, Analytics, Profilare) trebuie să fie **explicit, informat și separat**. Nu folosiți bifat implicit (pre-ticked boxes).

Tabel recomandat pentru auditul consimțământului (Consent Audit Trail):

```
CREATE TABLE user_consents (
    id BIGINT PRIMARY KEY AUTO_INCREMENT,
    user_id BIGINT NOT NULL,
    consent_type VARCHAR(50) NOT NULL, -- ex: 'marketing_email', 'analytics_cookies'
    is_granted BOOLEAN NOT NULL,
    granted_at TIMESTAMP NOT NULL,
    ip_address VARCHAR(45),
    user_agent TEXT,
    version VARCHAR(10) NOT NULL -- versiunea Politicii de Confidențialitate
);
```

5.2. SDK-uri terțe și Script-uri externe

Orice SDK integrat (Google Analytics, Facebook Pixel, Mixpanel, Hotjar) care colectează IP-uri sau comportament de navigare transmite date către terți. Încărcarea acestor script-uri pe frontend trebuie **blocată din punct de vedere tehnic** până la obținerea acordului prin bannerul de cookie-uri.

Checklist rapid de conformitate pentru Developer/DevOps

1. [ ] Exista HTTPS configurat și forțat pe toate domeniile/subdomeniile?
2. [ ] Sunt parolele stocate utilizând algoritmi siguri de hashing (Argon2id, bcrypt)?
3. [ ] Logurile de sistem sunt filtrate și nu conțin parole, token-uri sau PII?

4. [ ] Exista un mecanism (API / buton) de ștergere sau anonimizare a contului de utilizator?
5. [ ] Baza de date conține un audit trail pentru consimțământul acordat de utilizatori?
6. [ ] Backup-urile au o politică de retenție definită și sunt criptate at-rest?
7. [ ] Script-urile de analiză terță sunt blocate până la acceptarea explicita a cookie-urilor?