Ce ar trebui să știe inginerii de software despre GDPR?

Acest subiect este unul uriaș, astfel încât ne vom concentra exclusiv pe procesul de creare de noi soluții software. Este mult de spus despre asistența organizatorică și legalitatea sistemelor, dar ele sunt extrem de dependente ca punct de plecare. GDPR nu permite multe excepții de la reguli, astfel încât atât marile, cât și micile întreprinderi, organizațiile non-profit și toate organizațiile guvernamentale trebuie să cunoască principalele puncte-cheie.

Un punct-cheie al Regulamentului este dat de **transparența prelucrărilor datelor cu caracter personal** în raport de persoanele vizate. Când aveți un registru — de exemplu, o bază de date — care conține date de identificare personală, GDPR impune transparență în utilizarea acestora. Acest lucru înseamnă că persoanele ale căror date sunt colectate ar trebui să fie capabile de a afla ceea ce se colectează, în ce scop, cine are acces la date și cât timp se vor afla datele cu caracter personal în cadrul sistemelor. Pentru a face față cu această cerință, în mod firesc ar trebui să se cunoască toate aceste lucruri și să fie documentate. În paralel cu acest principiu, trebuie să se ofere un acces facil la datele cu caracter personal. Persoanele vizate ar trebui să poată verifica, corecta, exporta, muta și șterge datele lor la fel de ușor precum încredințarea lor.

Un alt subiect important este reprezentat de ***privacy by design/default***. *Privacy by default* înseamnă o mulțime de lucruri, dar, în esență, este menit a proteja datele cu caracter personal prin controale adecvate. Acest lucru necesită de obicei, de exemplu, piste de audit clare: cine, ce, când a făcut și mai ales cine are acces la datele cu caracter personal. În plus, ar trebui să se acorde o atenție sporită atunci când datele cu caracter personal sunt stocate și atunci când se află în tranzit între diferite straturi și se aplică metode de criptare adecvate pentru a evita scurgerea datelor cu caracter personal din sistem.

Ar trebui să existe, de asemenea, o bază legală pentru prelucrarea datelor cu caracter personal, ceea ce înseamnă, mai exact, aspectul care vă oferă dreptul de a colecta și de a prelucra informațiile. Baza legală pentru prelucrarea datelor cu caracter personal, de exemplu, ar putea fi o dispoziție legală care impune colectarea și stocarea datelor cu caracter personal pentru o perioadă de timp. Baza legală pentru prelucrarea datelor cu caracter personal poate fi un contract, un acord sau o tranzacție.

Puteți solicita consimțământul pentru a colecta și a prelucra date personale, dar GDPR impune cerințe suplimentare în acest caz. Nu este acceptabilă o casetă de selectare verificată deja cu o declarație ca *„Accept că informațiile mele pot fi utilizate în scopuri de marketing."* Acordul trebuie să fie clar, precis și ușor de înțeles și nu poate fi pre-stabilit. Ar trebui să fie la fel de ușor retragerea/revocarea consimțământului. Designerii de software nu pot decide niciuna dintre aceste chestiuni pe cont propriu, motiv pentru care trebuie să discute cu oricine deține cunoștințe în domeniu.

În cazul în care membrii echipei care construiesc software-ul au acces la datele personale în timpul procesului, aceștia devin persoane împuternicite de operatorul de date cu caracter personal și sunt supuși acelorași sancțiuni și responsabilități. Același lucru este valabil și pentru echipa de operațiuni, dacă are acces la bazele de date care conțin date cu caracter personal. Este însă posibil să construiți și să operați de cele mai multe ori sisteme fără accesarea datelor cu caracter personal ale clientului – operator de date cu caracter personal.

ATENȚIE!

Privacy by default înseamnă o mulțime de lucruri, dar, în esență, este menit a proteja datele cu caracter personal prin controale adecvate.

Recunoașterea informațiilor de identificare personală

GDPR este interesat doar de informații de identificare personală. GDPR nu se aplică în cazul datelor care nu sunt atașate unei persoane, cum ar fi datele despre produs sau informațiile contabile.

GDPR identifică două clase de date cu caracter personal. Există date care pot fi utilizate pentru a identifica o persoană, spre exemplu, CID, adresa de e-mail sau orice identificatori conectați direct la acestea, cum ar fi istoricul achizițiilor. Apoi, există date cu caracter personal speciale, cum ar fi informații medicale/sănătate, religie, orientare sexuală etc.

ȘTIAȚI CĂ?

Potrivit GDPR, *combinațiile de informații care nu pot fi unice în mod singular au potențial de a identifica un individ.* Deci datele cu caracter personal includ, de asemenea, identități care pot fi deduse din valori cum ar fi codul poștal, de călătorie, sau multiple locații, cum ar fi puncte de cumpărare. Seturile mici de date și combinațiile de valori rare pot face ca identificarea să fie mai ușoară.

De vreme ce orice informații anexate sau colectate de la o persoană vizată sunt protejate în conformitate cu GDPR, cele mai multe baze de date vor conține date cu caracter personal, cu unele excepții. Nu ar trebui protejate doar numerele de securitate socială și numerele cardurilor de credit.

Au existat o mulțime de discuții despre jurnalele de acces sau de auditare etc. care conțin adrese IP sau chei surogate. Acestea sunt date cu caracter personal? Sunt ele înregistrate? GDPR se extinde și la acestea? Cât de mult trebuie ele protejate? Acest tip de informații ar putea și ar trebui să fie protejate într-o anumită măsură, în funcție de cât de multe daune ar provoca o încălcare a datelor.

Proiectarea din momentul conceperii

Cel mai ieftin mod de a avea software conform cu GDPR este de a construi cerințele în interiorul său. Cât de cuprinzător ar trebui să se facă acest lucru depinde de nivelul de risc al sistemului special în cauză:

- ✓ Sistemul conține date cu caracter special?
- ✓ Sistemul conține informații care nu ating gradul de sensibilitate în sensul GDPR, dar ar fi jenant/periculos dacă ar fi publicate?
- ✓ Dacă cineva a publicat conținutul bazei de date, cât de mare este riscul pentru companie?
- ✓ Cât de mulți utilizatori există în baza de date?

Dacă există puțini utilizatori și informațiile pe care le colectează nu se încadrează în categoria celor sensibile sau dăunătoare, ați putea considera sistemul dumneavoastră ca având un risc mediu/scăzut chestiune dublată de efectuarea mai multor controale eficiente pentru a fi protejat. Pe de altă parte, dacă sistemul conține date sensibile pentru mulți utilizatori, ar fi de dorit să se aplice un sistem de protecție mai puternic.

IMPORTANT!

***Efectuarea unui audit este o cerință minimală.* Acesta evidențiază nu doar că ați efectuat controale, ci vă ajută să limitați daunele în cazul unei încălcări de date. După ce are loc orice încălcare a datelor cu caracter personal, cauzat fie de către un factor intern sau extern, primul lucru pe care trebuie să îl faceți este de a găsi *metoda care să poată evidenția utilizatorii afectați și datele care au fost accesate.* Aceste informații trebuie să fie raportate autorităților de supraveghere (ANSPDCP). În plus, aceștia sunt utilizatorii care ar trebui notificați despre încălcarea datelor cu caracter personal. Dacă nu aveți o asemenea metodă, ar însemna să se presupună că o încălcare a datelor cu caracter personal este posibil să îi fi afectat pe toți utilizatorii, precum și toate înregistrările existente în sistem.**

Un proces bun de auditare oferă, de asemenea, non-repudierea — cu alte cuvinte, acesta nu poate fi modificat/deteriorat nici chiar de către administratorii de sistem. Ați putea dori să utilizați piste de audit pentru a vedea datele din sistem încălcate, spre exemplu de către administratorul de sistem. Acest lucru s-a întâmplat înainte de și se va întâmpla din nou. Pistele de audit sunt, de asemenea, clasificate ca date cu caracter personal/identificatori: au o identitate unică și datele sunt conectate direct la ele.

IMPORTANT!

După traseele de audit, următoarea sarcină este *limitarea expunerii datelor*. Cel mai bun mod de a face acest lucru este de a limita datele care se colectează și durata stocării lor. Prin introducerea unui mecanism de arhivare/ștergere în software de la început, acest lucru poate fi documentat pentru utilizatori. Dacă se produce o încălcare a datelor cu caracter personal, aceasta poate afecta numai datele incluse în sistemul-țintă în acel moment. Multe sisteme continuă să colecteze toate datele, dar niciodată nu le elimină din sistem, chiar și atunci când datele devin învechite. GDPR încurajează să definiți în mod clar ciclurile de viață și documentarea datelor cu caracter personal. De asemenea, ar trebui să restricționați accesul la datele cu caracter personal numai la ceea ce este cu adevărat necesar. Acest lucru se impune mai ales pentru datele cu caracter personal sensibile.

Am menționat deja că ar trebui să aveți suficiente mecanisme de protecție pentru datele existente într-un sistem de baze de date sau fișier și care se mișcă printr-o rețea, în special la alte părți. Criptarea este eficientă, dar are punctele sale slabe. Cea mai puternică tehnologie de criptare: criptează devreme, securizează cheile și decriptează târziu. Din păcate, aceasta este o soluție complexă și costisitoare pentru a o pune în aplicare. La celălalt capăt al spectrului se află serviciile cloud, adesea simple și avantajoase, care pur și simplu criptează întreaga bază de date cu o casetă de selectare sau permite gestionarea cheilor și se efectuează criptarea pentru client. În timp ce este ușor, acest mecanism are de asemenea puncte slabe. Trebuie doar să găsiți ceea ce funcționează pentru companie, analiză care trebuie să aibă la bază o abordare bazată pe riscuri și pe sensibilitatea datelor.

Este demn de menționat faptul că mecanismele de anonimizare și pseudonimizare, vă pot ajuta în legătură cu testarea sau analiza datelor cu caracter personal. Anonimizarea elimină practic toate informațiile identificabile prin ștergere sau câmpuri mascate. Pseudonimizarea înlocuiește informații de identificare cu pseudonime, care de obicei păstrează identitatea separată în cuprinsul datelor. Ambele practici, cu toate acestea, sunt dificil de efectuat și pot fi imperfecte. Totuși, acestea sunt instrumente valoroase menționate în mod expres de GDPR.

Ați putea dori să revizuiți standardele de logare și liniile directoare. Este mai ușor în cazul în care vă asigurați că jurnalele nu conțin date cu caracter personal, în caz contrar, ele devin date cu caracter personal și de aici decurg toate implicațiile prevăzute de GDPR. Unele jurnale sunt atașate deja unor persoane: jurnale de acces și jurnale de audit, de exemplu. Dar nu includeți în acestea ID-uri de utilizator, nume sau valori similare. Este bine să se separe în mod clar jurnalele care pot fi legate de persoane fizice de jurnalele care nu poate fi legate de persoane fizice, dar conțin informații generale ale sistemului.

Documentați-vă sistemul

Un aspect important prevăzut de Regulament este de a fi în măsură să **demonstrați conformitatea.** Puteți face acest lucru prin certificate care, la rândul lor, beneficiază de documentarea sistemelor sau de documen-

ATENȚIE!

Criptarea este eficientă, dar are punctele sale slabe. Cea mai puternică tehnologie de criptare: criptează devreme, securizează cheile și decriptează târziu.

tație folosită pentru furnizare, care poate varia pe baza mai multor factori. Dar există unele documente suplimentare, care ar fi utile și anume:

- indicați datele cu caracter personal în cadrul sistemului;
- indicați circuitul datelor cu caracter personal colectate;
- indicați toate părțile care prelucrează datele cu caracter personal;
- indicați baza legală de prelucrare;
- informați persoanele vizate cu privire la drepturile lor și explicați-le cum își pot exercita drepturile prevăzute de Regulament în favoarea lor.

Persoană împuternicită sau nu?

Când lucrați la un proiect de software sub imperiul responsabilităților instituite de GDPR, trebuie să răspundeți la o întrebare importantă: aveți intenția să fiți o persoană împuternicită de operator sau nu? În mod implicit, ar fi de dorit să nu fiți o persoană împuternicită de operator, deoarece fiind unul sunteți pasibil a fi răspunzător pentru orice sancțiuni. Pentru a evita regimul sancționatoriu prevăzut de GDPR, pur și simplu asigurați-vă să nu aveți și să nu puteți accesa niciun fel de date cu caracter personal sau identifictaori ale acestora. Trebuie să vă asigurați că acest aspect este prevăzut în mod clar în orice contract încheiat. Ar putea fi dificil de a evita prelucrarea datelor cu caracter personal, deoarece datele personale pot fi ascunse în fișiere-jurnal, medii de testare și orice corecții de urgență din mediul de producție. Dar dacă doriți să evitați o potențială răspundere trebuie să aveți în vedere acest lucru. **Protejați-vă de datele cu caracter personal. Protejați datele cu caracter personal la care aveți acces**.

O altă cale este aceea de a îmbrățișa statutul de persoană împuternicită de operator. Acest lucru vă permite să aveți acces liber la datele cu caracter personal, atâta timp cât vă documentați activitatea, aveți o bază legală pentru prelucrare și acest acces este bine definit și delimitat. Acest lucru vă face în mod clar responsabil, așa că trebuie să fiți atent la orice sancțiuni. Dar acesta este traseul de urmat dacă aveți absolută nevoie de acces la baza de date ce conține date cu caracter personal.

Cele mai multe proiecte software necesită expunere la datele cu caracter personal și cu siguranță aceasta este calea recomandată de urmat — dar în acest caz veți avea nevoie de noi competențe și instrumente.

IMPORTANT

În ceea ce privește legalitatea prelucrării datelor cu caracter personal de către angajator prin GPS a angajatului, apreciem că pot fi incidente următoarele situații prin raportare la diversitatea practicii în materie: (a) consimțământul șoferului (persoanei vizate); (b) executarea unui contract; (c) interesul legitim al angajatorului.

Spre exemplu:

1. Şoferul este plătit în funcție de numărul de kilometri parcurși, respectarea timpilor etc. În acest caz monitorizarea prin GPS ar trebuie să fie reglementată și în contractul de muncă, caz în care considerăm că nu este nevoie de consimțământ, baza legală pentru prelucrare fiind reprezentată de executarea contractului de muncă.
2. O companie închiriază mașini sau are un serviciu de car sharing. În acest caz, pe lângă executarea unui contract există și interesul legitim al organizației, respectiv prevenirea fraudei/furtului.
3. Dacă se permite utilizarea autovehiculului în scopuri personale, apreciem că persoana vizată trebuie să aibă înainte de toate posibilitatea ca sistemul de monitorizare să fie oprit (sau o formă de opt-out).

Cu toate acestea dacă operatorul de date își întemeiază decizia de prelucrare a datelor cu caracter personal pe interesul său legitim, acesta poate fi aplicabil doar în condițiile în care nu prevalează asupra drepturilor și libertăților fundamentale ale persoanei vizate. În situația contrară, credem că ar trebui solicitat consimțământul persoanei vizate. În raport de aceste aspecte, apreciem că modelul identificat de către dumneavoastră pe website este aplicabil în situații de acest tip și vă recomandăm să îl aveți în vedere doar pentru astfel de situații. Recomandăm, de asemenea, să consultați considerentele cauzei Bărbulescu c. României cu privire la criteriile necesar a fi avute pentru respectarea dreptului la viața privată a salariatului și limitele de apreciere a acestuia.