SMART <GDPR> CITY

George Simion, CISO KMG Rompetrol și
membru colaborator ANSSI

Introducere

Pentru început, ce înseamnă “Smart City” ?

Dacă ne uităm la abordarea British Standard Institute, un oraș devine “mai inteligent” dacă reușește să integreze efectiv sistemele fizice, digitale și resursele umane pentru a oferi cetățenilor săi un viitor durabil și prosper.

Pe de altă parte, Universitatea Tehnică din Berlin consideră un oraș “smart” ca o sumă de sisteme, așezări urbane și oameni.

Având în minte toate acestea, putem spune că un oraș “smart” poate fi definit ca un oraș în care noi tehnologii sunt implementate, unde oamenii pot accesa ușor informații sau sisteme, unde informația – data – este utilizată peste medie.

“Smart” poate reprezenta un aspect al oricărei componente a unui oraș, de la serviciile medicale și de educație la transport, Securitate (poliție, pompieri) sau utilitățile publice generale (apă, energie electrică etc.). Capabilitățile aduse de tehnologie în aceste arii sunt variate și fac fiecare arie în parte mai eficientă. De exemplu, rețelele Wi-Fi publice din spațiile unităților administrative pot îmbunătăți nivelul de comunicare, pot facilita identificarea nevoilor fiecărei persoane în parte și estima necesitățile acesteia. Capabilitățile de comunicare de tip IoT, utilizate în transporturi sau în serviciile de salubrizare, pot îmbunătăți calitatea serviciilor și reduce costurile, sistemele de telemetrie pot optimiza modul de livrare (și consum) a apei potabile sau a energiei.

Noul cadru legislativ, Regulamentul general privind protecția datelor (GDPR), care va intra în vigoare din 25 Mai, va aduce un nivel în plus de complexitate privind modul în care informațiile sunt colectate, utilizate și nu în ultimul rând stocate.

Regulamentul general privind protecția datelor – GDPR

GDPR este în aceste zile un acronim foarte uzual și motivul principal pentru care este atât de uzual este datorat faptului că această lege nouă aduce un nivel foarte ridicat de amenzi. Totuși, principiile puse în discuție de lege existau deja în cadrul general legislativ, însă într-o formă diferită. Noua lege aduce două schimbări semnificative când vine vorba de proiecte de tip “oraș inteligent”; prima schimbare o reprezintă delimitarea activităților de interes public (așa cum sunt ele menționate în Art. 6 al Regulamentului) și activitățile private; iar a doua schimbare o reprezintă valorile semnificative de penalitate financiară în cazurile de utilizare excesivă a datelor sau pierderea acestora.

Utilizarea excesivă a datelor poate fi definită fie prin colectare și utilizarea acestora fără acordul persoanei în cauză (“subiectul” după cum este denumit în Regulament) sau prin procesarea datelor în alte scopuri decât cele declarate și pentru care s-a obținut acord de procesare.

Acordul persoanei identificate prin aceste date este un element foarte important al Regulamentului iar descrierea lui este foarte detaliată în textul legislativ – acordul trebuie să fie primit într-un mod concis, într-o formă ușor de înțeles și folosind un vocabular simplu, cu scop explicit și limitat în timp. În plus, în momentul în care se obține acest acord trebuie adus la cunoștința persoanei în cauză și dreptul de a solicita actualizarea sau ștergerea datelor cu caracter personal (termenul utilizat în textul legislativ fiind “dreptul de a fi uitat”).

Conform Art .11 din Regulament, dacă scopul utilizării datelor nu presupune un nivel de detaliu care să permită identificarea ulterioară a persoanei atunci nici procesatorul nu are obligația de a colecta, menține și procesa informații suplimentare doar pentru a fi conform cu legislația.

În această perioadă, la nivelul sistemelor IT precum și la nivelul proceselor de lucru, se desfășoară un proces de analiză și audit din perspectiva GDPR (proces denumit Analiza de impact asupra protecției datelor – DPIA). Însă companiile nu ar trebui să se oprească doar la acest proces punctual deoarece GDPR nu este un simplu proiect ci este mai degrabă un program, un proces continuu la care sistemele și procesele de lucru trebuie să fie aliniate în permanență. Dacă avem în vedere costurile unei implementări ulterioare a cerințelor GDPR, precum și contextul unor modificări viitoare în arhitectura sistemelor, procesatorul datelor ar trebui să aibă în vedere capabilități de pseudonimizare sau reducere la minim a nivelului de date colectate. Aceste măsuri vor asigura corectitudinea procesării datelor în vederea respectării Regulamentului și protejării drepturilor persoanelor încă din momentul punerii în producție a sistemelor noi.

Pierderea datelor poate avea loc în multe feluri, iar DPIA este un moment foarte bun de a le analiza. De exemplu, datele pot fi pierdute din cauza securității serviciilor (de exemplu în anul 2017 Equifax a pierdut datele a milioane de persoane datorită unei vulnerabilități de aplicație), pot fi pierdute din cauza modului în care sunt manipulate (de exemplu în ianuarie 2018 Universitatea Coventry a recunoscut faptul că date ale studenților au fost făcute publice prin simpla atașare eronată a unui fișier la un email) și nu în ultimul rând, datele pot fi pierdute prin administrarea defectuasă a sistemelor – fișierele de log și fisierele de backup pot conține date cu caracter personal la fel de bine precum bazele de date în sine.

GDPR și Proiectele Smart City

Acum, după ce am trecut în revistă terminologia utilizată atât în proiecte „Smart City” cât și în legislația GDPR, haideți să vedem cum se vor intersecta acestea.

În primul rând autoritățile și furnizorii de utilități publice vor trebui să nominalizeze o persoană responsabilă cu protecția datelor (Data Protection Officer – DPO), persoană care va monitoriza îndeplinirea cerințelor Regulamentului în cadrul organizației sale. DPO va trebui să se asigure de conformarea proceselor interne la cadrul legislativ (evidența punctelor în care sunt colectate datele cu caracter personal, evidența activităților de procesare a acestor date și a conformității procesării cu scopul declarant și nu în ultimul rând asigurarea securității fizice și logice a acestor date). Nici procesele externe, de interacțiune cu autoritățile sau persoanele ale căror date sunt procesate, nu trebuie uitate de către DPO, acesta urmând a întreține un sistem de administrare a acordurilor primite, precum și un sistem de management a solicitărilor și plângerilor cu referire la datele cu caracter personal.

Cele mai uzuale servicii digitale care pot fi utilizate și furnizate de autorități și de entitățile de furnizare a utilităților publice sunt portalurile web sau rețelele de tip Wi-Fi, însă pot fi întâlnite și sisteme complexe (Centre de comandă centralizată a sistemelor orașului).

Pentru portalurile web, din perspectiva GDPR, este necesar acordul de colectare și procesare a datelor cu caracter personal deoarece:

- Sunt utilizate cookies (fișiere mici care sunt descărcate la vizitarea unei pagini web și care conțin informații despre vizitator, informații care pot conduce la crearea unui profil al vizitatorului – aceste fișiere sunt menționate în Regulament în cadrul Recitalului Nr. 30)
- Sunt utilizate formulare (fiecare formulare din portalul web trebuie să specifice scopul pentru care sunt solicitate informațiile și de asemenea este recomandat să nu existe setat ca implicit acordul de colectare și procesare)
- Sunt utilizate elemente de securizare (este recomandat să se afișeze mesaje prin care să se comunice dacă informația va fi transmisă într-un mod securizat sau nu, prin internet)
- Sunt emise anunțuri (anunțurile – en. newsletters – au la bază acorduri de utilizare a datelor personale în scouri de marketing iar persoana în cauză trebuie să poată accesa cu ușurință opțiunea de modificare/retragere a acestor acorduri).

Rețelele Wi-Fi publice intră în scopul Regulamentului datorită transferului de date de profil (informații cu caracter personal sunt colectate la autentificarea într-o rețea Wi-Fi); datorită înregistrării istoricului acțiunilor utilizatorului (existența istoricului trebuie făcută cunoscută utilizatorlui) dar și datorită schimburilor de date cu alți parteneri de afaceri (dacă datele cu caracter personal sunt utilizate în relația cu alte companii acest aspect trebuie adus la cunoștința persoanei în cauză și trebuie obținut acordul în acest sens).

Echipamentele de tip IoT aduc capabilități noi în toate componentele unei infrastructuri de tip “smart city”. De exemplu în cazul unei soluții de parcare inteligentă, șoferii pot fi ghidați spre cel mai apropiat loc disponibil, numărul de înmatriculare al autoturismului poate fi identificat în vederea calculului automat al sumei de plată pentru parcare și nu în ultimul rând se poate procesa plata serviciilor din contul soferului. În acest exemplu următoarele elemente sunt afectate de GDPR:

- Camerele web (pentru înregistrarea video a șoferului și pentru identificarea numărului de înmatriculare al autoturismului)
- Sistemul de management al parcării (pentru crearea unui profil de utilizator, pentru procesarea sumelor de plată și eventual pentru exportul acestora către sisteme externe de plăți)
- Automate de plată (datorită procesării datelor financiare ale persoanei în cauză)
- Aplicații web (datorită creării de profile utilizatori, datorită conectării profilelor de utilizatori cu sisteme/conturi bancare și cu administațiile financiare)

Aceste detalii despre datele cu caracter personal trebuie aduse la cunoștința persoanelor care utilizează parcarea atât la intrarea în parcare (fizic) cât și în aplicațiile web, în așa fel încât decizia de a utiliza sau nu serviciile să poată fi luată în cunoștință de cauză.

Centrele de comandă centralizată a orașelor reprezintă infrastructuri dedicate în vederea concentrării mai multor activități într-un singur punct și cu scopul de a permite aplicarea anumitor decizii foarte repede. Un astfel de centru are următoarele capabilități:

- Sistem complex de camere video
- Integrează resurse și permite conlucrarea între mai multe servicii simple
- Analiză inteligentă a informațiilor globale și propunerea de decizii
- Administrarea traficului de mașini

Toate aceste capabilități au la bază utilizarea la comun a datelor obținute de mai multe companii, situație în care acordul explicit nu este necesar întrucât rolul primar al autorităților este acela de a ține orașul funcțional și sigur. Acest aspect este tratat atât în cadrul Regulamentului în Recitalul 35 cât și prin Directiva Parlamentului European nr. 2011/24/EU.

În situațile în care o companie condiționează livrarea unui serviciu de procesarea datelor persoanei consumatoare, acordul poate fi considerat abuziv și invalid. Însă, dacă procesarea este necesară pentru serviciul în sine, aspect definit în Regulament prin "necesar pentru executarea unui contract" la articolul 6, aliniatul 1, litera b, atunci acordul este considerat implicit prin semnarea contractului în sine.

Concluzii

GDPR nu are scopul de a opri servicii sau de a bloca implementarea unor proiecte noi, însă urmărește să crească gradul de transparență în ceea ce privește utilizarea datelor cu caracter personal. Cele mai multe aspecte existau în legislație și înainte de apariția GDPR (Directiva Europeană 95/46 privind Protecția Datelor de exemplu) însă în acest moment acestea sunt explicate și detaliate foarte bine.

Proiectele de tip "Smart City" continuă, și vor continua, să crească, însă o atenție deosebită va fi asupra modului de utilizare a datelor cu caracter personal și a modului de colaborare între entitățile autorităților publice.

Surse de date:

https://gdpr-info.eu
https://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/
http://www.smartcity.tu-berlin.de/smart-city-definition-an-der-tu-berlin-smart-city-platform/
https://www.coventrytelegraph.net/news/coventry-news/revealed-university-under-investigation-after-14201206