

# **Dane przestrzenne a RODO – czy lokalizacja to informacja wrażliwa?**

Mało kto zdaje sobie sprawę, że ponad 80% danych ma swoje odniesienie w przestrzeni. Dane przestrzenne stanowią fundament działania wielu firm i organizacji, a także usług i aplikacji. Jednym z wyróżników tych danych jest to, że w większym stopniu niż inne mogą ujawnić wrażliwe informacje na temat poszczególnych osób. Przyczynia się do tego rosnąca popularność mobilnego internetu, który umożliwia zbieranie informacji o położeniu osób i urządzeń. Z tego powodu znaczenie danych lokalizacyjnych zostało dostrzeżone przez Parlament Europejski i Radę UE i uwzględnione w rozporządzeniu RODO.

Definicja danych lokalizacyjnych generowanych przez użytkowników aplikacji mobilnych zawarta jest w regulacji PECR (Privacy and Electronic Communications Regulations). Są to wszystkie informacje, przetworzone w komunikacyjnej sieci łączności elektronicznej lub za pomocą elektronicznej usługi komunikacyjnej, wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznej usługi łączności elektronicznej, w tym dane o:

- szerokości, długości lub wysokości tego urządzenia,
- kierunku przemieszczania się użytkownika,
- czasie zarejestrowania informacji o lokalizacji.

Innymi słowy, dane lokalizacyjne to informacje zebrane przez aplikację lub dostawcę usług o tym, gdzie urządzenie mobilne użytkownika znajdowało się w określonym czasie.

**Powiedz mi gdzie mieszkasz, a powiem Ci kim jesteś**

Zgodę na dostęp do informacji o naszej lokalizacji najczęściej

wyrażamy w momencie instalacji aplikacji na naszym urządzeniu mobilnym. Często nie zdajemy sobie jednak sprawy, co dzieje się z tymi danymi, czyli: w jaki sposób są one zbierane, przetwarzane czy udostępniane. Wbudowane nadajniki GPS wykorzystywane są m.in. przez aplikacje mapowe, aplikacje do zamawiania przejazdów, do łączenia kierowców i pasażerów czy aplikacje fitness, monitorujące trasy i intensywność wysiłku fizycznego.

Dyskusyjne jest natomiast zbieranie danych o lokalizacji przez takie serwisy jak Facebook czy Instagram, których działanie nie opiera się w głównej mierze na danych lokalizacyjnych. Aplikacje te śledzą bowiem nasze położenie w sposób domyślny, nawet gdy nie są używane. Do czego są więc im te dane potrzebne? Otóż na podstawie informacji o lokalizacji firmy są w stanie planować skuteczniejsze, spersonalizowane reklamy. W zamian użytkownik otrzymuje dokładniejsze sugestie odnośnie potencjalnych znajomych lub wydarzeń w najbliższej okolicy.

Permanentne monitorowanie aktywności użytkowników przy ograniczonej przejrzystości informacji o tym, do czego wykorzystywane są zdobyte dane, wzbudziło obawy odnośnie prywatności zarówno użytkowników, jak i organów regulacyjnych. Tę kwestię podjęły m.in. Parlament Europejski i Rada Unii Europejskiej, która określiła zbiór zasad i regulacji mających na celu poprawę przejrzystości w obszarze ochrony danych osobowych.

*„Dane lokalizacyjne nie zawsze są związane z danymi osobowymi, ponieważ wszystko zależy od kontekstu i sposobu ich wykorzystywania. Użycie danych np. do optymalizacji procesów w logistyce nie narusza zasad prywatności. Inaczej będzie natomiast w sytuacji, w której dane wrażliwe są wykorzystywane m.in. do monitorowania pacjentów czy dziecka. Szczególne wyzwania dotyczą w tym kontekście podmiotów zbierających informacje na temat użytkowników, które pochodzą bezpośrednio z urządzeń mobilnych. Dotyczy to przede wszystkim wykorzystania nadajników GPS, ale także Bluetooth czy Wi-Fi” –*

dodaje Małgorzata Grzywacz, dyrektor marketingu w firmie Esri Polska.

## **Dane przestrzenne – dane wrażliwe**

### **1. Lokalizacja może być identyfikatorem**

Głównym wyzwaniem związanym z wykorzystywaniem geodanych jest możliwość powiązania ich z konkretnym użytkownikiem. Z tego powodu kluczowa jest anonimizacja, czyli zastosowanie procesu uniemożliwiającego odkrycie tożsamości użytkownika. W kontekście informacji przestrzennych nie jest to takie proste, jak w przypadku innych informacji zbieranych i przechowywanych przez firmy. Nie wystarczy eliminacja czynnika identyfikującego tożsamość danej osoby. Codzienne czynności, takie jak np. podróże do pracy, zdradzają przykładowo miejsce naszego zamieszkania.

### **2. Lokalizacja zawiera poufne informacje**

Wrażliwe dane osobowe są terminem używanym w RODO do opisu informacji wymagających szczególnej ochrony. Obejmują takie informacje, jak pochodzenie etniczne, przekonania religijne, polityczne czy światopoglądowe, dane dotyczące zdrowia lub orientacji seksualnej danej osoby. Przykładowo: częste wizyty w szpitalu lub w miejscach, których odbywają się spotkania wyborcze danej opcji politycznej mogą ujawniać wrażliwe informacje. Po raz kolejny pojawia się konieczność anonimizacji takich danych.

### **3. Lokalizacja tworzy wzorce**

Gromadzenie informacji przestrzennych może przekazywać istotne dane i tworzyć wzorce, nawet jeśli informacje te są skutecznie anonimizowane. Co prawda wzorce te zawierają wiele istotnych danych dla firm, jednak istnieje niebezpieczeństwo, że mogą zostać wykorzystane niezgodnie z ich przeznaczeniem. Na przykład na początku 2018 roku jedna z firm obsługujących aplikację dla sportowców ujawniła mapy ciepła, które wskazały

lokalizację amerykańskich baz wojskowych rozmieszczonych w odosobnionych miejscach. Mapa aplikacji wizualizowała szlaki biegowe sportowców – w tym żołnierzy – na całym świecie, co pozwalało na łatwe zlokalizowanie newralgicznych obszarów, na których istniały tajne bazy. Sprawa ta wywołała olbrzymie kontrowersje na temat wpływu danych lokalizacyjnych na funkcjonowanie firm, ich odpowiedzialności, zastosowania odpowiednich protokołów bezpieczeństwa oraz zakresu zgody użytkowników na udostępnianie informacji.

## **Gdzie to RODO?**

Z powyższych powodów ochrona danych lokalizacyjnych i dostęp do nich podlega tym samym regulacjom, co inne wrażliwe dane osobowe. W ramach rozporządzenia RODO mamy m.in. prawo do wglądu do zgromadzonych przez kogokolwiek tego typu informacji na nasz temat i usunięcia ich z bazy danych. Przetwarzający, zwani również procesorami danych, muszą w jawny i przejrzysty sposób powiadamiać swoich użytkowników o praktykach dotyczących ich danych. Podejście to powinno gwarantować, że operatorzy danych podejmą środki niezbędne do bezpiecznego gromadzenia, przetwarzania i przechowywania danych.

RODO określa również specjalne zasady stosowane w stosunku do procesorów wrażliwych danych. Obejmuje to wytyczne dotyczące oceny danych, wymuszając na organizacjach powołanie specjalistów ds. ochrony danych osobowych. W rozporządzeniu znalazły się również zapisy dotyczące znaczenia zgody. Po jego wprowadzeniu zasady dotyczące przechowywania danych muszą być jasno sformułowane na etapie instalowania i późniejszego używania aplikacji.

Podsumowując: po wprowadzeniu w życie rozporządzenia o ochronie danych osobowych kluczowa dla organizacji powinna stać się kwestia zrozumienia danych lokalizacyjnych i ich odpowiednia ochrona. – Rozporządzenie RODO podnosi standardy bezpieczeństwa i upraszcza komunikację na temat tego, w jaki sposób są one wykorzystywane. W dalszej perspektywie lepsze

zrozumienie i przejrzystość różnych informacji oraz konsekwencje ich wykorzystywania niosą korzyści zarówno dla organizacji, jak i użytkowników, których te dane dotyczą.