

Cykl GIODO radzi...;)



GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Jak chronić dane osobowe
podczas wakacji?

GIODO radzi... ;)

Co na Twój temat wie Twój telefon komórkowy?

W związku z coraz większą popularnością aplikacji mobilnych wykorzystujących technologię geolokalizacji oraz wirtualnej rzeczywistości (jak np. Pokemon Go, HERE City Lens Corinth Micro Anatomy Augmented, dostępnych także w Polsce na urządzenia mobilne), Generalny Inspektor Ochrony Danych Osobowych zachęca do ostrożnego i bezpiecznego użytkowania urządzeń przenośnych.

Oto kilka wskazówek GIODO dotyczących bezpiecznego korzystania ze smartfonów:

- **Czytaj regulaminy i polityki prywatności.** W pierwszej kolejności zalecamy wszystkim użytkownikom zapoznanie się z polityką prywatności takich aplikacji oraz wszelkimi udostępnianymi komunikatami, z których dowiedzieć się można do jakich danych będzie miała dostęp konkretna aplikacja i w jakim celu będzie je wykorzystywać. W tym zakresie szczególną uwagę zwracamy na postanowienia regulaminów dotyczące przekazywania za pośrednictwem aplikacji danych osobowych do państw
- **Rozważnie korzystaj z nieznanych sieci bezprzewodowych Wi-fi.** Należy także pamiętać, że niektóre z aplikacji mobilnych (ale także stron internetowych oraz sieci Wi-Fi) mogą podczas korzystania z nich gromadzić informacje o lokalizacji użytkowników. Sprawdź jakie dane globalizacyjne są przesyłane przez aplikacje
- **Ustal jakie dane osobowe udostępniają zainstalowane aplikacje.** Sprawdź w urządzeniu mobilnym zakładkę Prywatność i dowiedz się jakie informacje o sobie udostępniasz. Z uwagi na szeroki zakres informacji gromadzonych na urządzeniu, jaki bardzo często wiąże się z użytkowaniem aplikacji, zachęcamy do refleksji czy na pewno chcemy by dana aplikacja miała uprawnienia np. do SMS, fotografii, filmów, email, kontaktów, czatów itp.
- **Nie klikaj podejrzanych linków, nie przeglądaj podejrzanych stron.** Stosuj tryb prywatny w przeglądaniu stron w celu minimalizacji gromadzonych na urządzeniu mobilnym informacji np. o lokalizacji, o odwiedzanych stronach itp.
- Jeśli to możliwe **stosuj wbudowane w urządzeniu oprogramowanie umożliwiające uruchomienie trybu prywatnego** w celu oddzielenia

danych prywatnych od służbowych lub innych informacji .

- Gry i aplikacje oparte na modelu tzw. rozszerzonej rzeczywistości mogą także rejestrować m.in. **wizerunki innych osób** poprzez użycie kamery aparatu. Jeśli to możliwe, należy unikać fotografowania osób trzecich w trakcie korzystania z aplikacji.
- **Chroń swoje dane do logowania** oraz wykonuj regularną zmianę trudnego do odgadnięcia hasła.
- **Aktualizuj oprogramowanie.** Korzystaj tylko z oprogramowania z legalnego źródła. Nie wykonuj Jailbreaking z zainfekowanym oprogramowaniem systemowym. Stosuj oprogramowanie chroniące twoje urządzenie (antywirus, Firewall, anty spam, itp.).
- **Każdy powinien również znać przysługujące mu prawa** tak, by był w stanie skutecznie reagować na wszelkie naruszenia jego prywatności w tym przypadki przetwarzania jego danych osobowych bez podstawy prawnej.

Zagadnieniem ochrony danych osobowych w urządzeniach przenośnych zajmowała się także Grupa Robocza Art. 29 - zachęcamy do zapoznania się z następującymi opiniami Grupy:

- [Opinia 13/2011 w sprawie usług geolokalizacyjnych w inteligentnych urządzeniach przenośnych](#),

- [Opinia 2/2013 w sprawie aplikacji mobilnych](#).

24-08-2016

- [Udostępnij](#)
- [Drukuj](#)
- [PDF](#)

[Wszystkie aktualności](#)