Źródło: <https://uodo.gov.pl/>

5 wskazówek, jak bezpiecznie korzystać z aplikacji mobilnych



**Moda na aplikacje mobilne nie jest niczym nowym. UODO od lat przypomina, że korzystanie z nich nie powinno usypiać naszej czujności. Bezrefleksyjne korzystanie z wielu nowoczesnych narzędzi może narazić nas na utratę naszych danych, co czasem przekłada się na duże problemy.**

Jednego dnia media społecznościowe „zalały” zdjęcia przerobione przez aplikację FaceApp. A następnego pojawiły się ostrzeżenia co do tej aplikacji. Chodzi nie tylko o to, że zdjęcia są przesyłane na serwery w jednym kraju, a tam mechanizmy sztucznej inteligencji dodają do wizerunku kilkadziesiąt lat.

Często aplikacje mobilne wymagają szerokiego dostępu do różnych zasobów w naszych smartfonach, tym samym szerokiej wiedzy o ich użytkownikach, takich jak dostęp do połączeń sieciowych, czy do pamięci, na której zostanie zapisany plik. Nie rzadko korzystają także z analizy naszych kontaktów, czy innych danych wrażliwych znajdujących się w naszych smartfonach.

Problem w tym, że czasami uprawnienia aplikacji są przedstawione ogólnie i de facto nie wiadomo, czy takie dostępy nie są wykorzystywane także w innych celach. Warto też np. zastanowić się, czy aplikacja z latarką potrzebuje dostępu do naszych kontaktów, a układanie puzzli musi śledzić nasze położenie. Dlatego przypominany 5 najważniejszych zasad, na temat bezpiecznego korzystania z aplikacji mobilnych.

**I Zwracaj uwagę na to do czego w Twoim telefonie chce mieć dostęp aplikacja**

Przed instalacją nowej aplikacji należy dokładnie przeanalizować, do jakich danych i funkcji naszego urządzenia chce mieć ona dostęp. Niektóre aplikacje domagają się dostępu do: informacji o naszej lokalizacji, zdjęć, kontaktów czy dokumentów. Watro wówczas zastanowić się, jaki jest cel dostępu do poszczególnych funkcji. Czy dając nieograniczony dostęp, np. do pamięci telefonu i naszych kontaktów, nie narazimy na utratę nie tylko swoich danych, ale i danych naszych znajomych. Takie aplikacje mogą niekiedy wysłać dodatkowe dane o nas bądź nieustannie śledzić naszą lokalizację.

Niektóre funkcje w aplikacjach są niezbędne do poprawnego ich działania, np. mapy i programy do nawigacji muszą korzystać z danych geolokalizacyjnych, by wskazać nam drogę do celu.

**II Pamiętaj, że zgodnie z RODO administratorzy muszą minimalizować przetwarzane dane**

Przy instalacji aplikacji zwróć uwagę, czy zakres przekazywanych za jej pośrednictwem danych na Twój temat jest adekwatny do celu, w jakim powstała dana aplikacja. Przykładowo oprogramowanie odpowiadające za skanowanie kodów QR albo czytnik e-booków nie potrzebują dostępu do Twoich kontaktów czy informacji o lokalizacji.

**III** **Dokładnie czytaj wszelkie informacje od producenta na temat aplikacji**

Jeżeli do działania aplikacji konieczne jest przetwarzanie danych osobowych, to administrator powinien spełnić wobec nas obowiązek informacyjny. RODO wymaga, by o wszelkich zasadach przetwarzania danych osobowych poinformował nas w sposób przejrzysty i zrozumiały, w zwięzłej formie, jasnym i prostym językiem.

Z informacji przekazywanych przez twórcę aplikacji możemy dokładnie poznać jego cele i zakres danych, jaki zamierza przetwarzać i w jakich celach.

**IV Zastanów się, czy na wszystko się chcesz zgadzać**

Instalując aplikacje mobilne, nie tylko godzimy się na wykorzystanie naszych danych, które są potrzebne do ich prawidłowego działania. Niekiedy twórcy takiego oprogramowania chcą pozyskać od nas więcej zgód, np. w celach marketingowych, wyświetlania nam spersonalizowanych reklam, powiadamiania nas o sklepach czy punktach usługowych w pobliżu miejsc, w których się w danym momencie znajdujemy.

Dobrze się zastanówmy zanim udzielimy takich dodatkowych zgód na przetwarzanie naszych danych w określonych celach. Co prawda RODO pozwala nam w dowolnym momencie wycofać zgodę na przetwarzanie naszych danych, ale sprawdźmy też, czy jest to równie łatwe, jak jej udzielenie.

**V Stosuj zasadę ograniczonego zaufania**

Pamiętaj, że nie wszyscy twórcy aplikacji rzetelnie informują o ich działaniu i sposobach wykorzystania naszych danych. Co i raz na światło dzienne wychodzą informacje, że niektóre aplikacje śledzą użytkowników i analizują ich zachowania bez ich wiedzy. Trudno się przed tym ustrzec całkowicie, ale można zminimalizować ryzyko i np. nie instalować aplikacji z niepewnych źródeł, które nie pochodzą z oficjalnych kanałów dystrybucji. Warto też śledzić doniesienia medialne nt. aplikacji mobilnych.

Jeżeli masz wątpliwości co do zakresu przetwarzanych danych przez aplikację, to skontaktuj się z jej twórcą. W przypadku braku reakcji z jego strony lub pozostawiania pytań bez odpowiedzi, bezpieczniej jest zrezygnować z takiej aplikacji i np. poszukać innej o podobnych funkcjach.

Jeżeli masz podejrzenie, że dana aplikacja bezprawnie wykorzystuje Twoje dane, skontaktuj się z jej administratorem. Warto również powiadomić o naszych podejrzeniach oficjalny kanał dystrybucji tej aplikacji, np. AppStore – często po takich zgłoszeniach znacznie wnikliwiej analizują działanie aplikacji, co do której pojawiają się wątpliwości. Możesz również zgłosić bezprawne przetwarzanie Twoich danych do Prezesa UODO.

Problematyka ingerencji aplikacji i nowoczesnych urządzeń w sferę naszej prywatności i zagrożeń związanych z nowymi technologiami nie jest nowa. A unijne organy ochrony danych osobowych od lat dyskutują na ten temat i podejmują działania mające na celu zapewnienie większej ochrony danych osobowych i uświadamiania obywateli o zagrożeniach. Przykładem jest podpisanie Deklaracji Warszawskiej podczas obrady 35. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności i przyjęcie rezolucji poświęconych m.in. profilowaniu, śledzeniu w sieci.

Również Grupa Robocza Art. 29 (zastąpiła ją Europejska Rada Ochrony Danych Osobowych) wydawała opinie nt. aplikacji na urządzenia inteligentne oraz w sprawie systemów rozpoznawania twarzy.