UODO radzi: Zadbaj, by twój telefon był przyjacielem, a nie szpiegiem!

Zadbaj, by twój telefon był przyjacielem, a nie szpiegiem

Podczas wakacji częściej niż zazwyczaj korzystamy z różnego rodzaju aplikacji, które mogą być nam pomocne w podróży czy uprawianiu sportu. Jeśli jednak instalując je, nie zachowamy należytej ostrożności, nasz telefon lub smartwatch z przyjaciela łatwo może stać się szpiegiem. Warto więc zwracać uwagę, m.in. na to, jakie dane zbierają aplikacje i na co się godzimy przy ich ściąganiu – przestrzega dr Edyta Bielak-Jomaa, prezes Urzędu Ochrony Danych Osobowych.

Przyłączając się jak co roku do organizowanej przez Urząd Ochrony Konkurencji i Konsumentów akcji „Przed wakacjami – co warto wiedzieć?”, prezes Urzędu Ochrony Danych Osobowych radzi jednocześnie, by podczas wakacji poświęcić czas na dokonanie przeglądu zainstalowanego oprogramowania pod kątem ochrony prywatności.

Telefon komórkowy czy smartwatch to dziś narzędzia, które oferują nam wiele użytecznych funkcji. Służą nie tylko komunikacji, ale dzięki zainstalowanym na nich aplikacjom także rozrywce, ułatwiają załatwienie codziennych spraw, poruszanie się, wspomagają aktywność fizyczną. Te z pozoru niewinne gadżety, niekiedy – czego nie zawsze jesteśmy świadomi – zbierają o nas bardzo dużo informacji, które bywają zbędne do świadczenia usługi, z której korzystamy. Tymczasem tak być nie powinno, zwłaszcza teraz, gdy do przetwarzania danych osobowych zastosowanie mają przepisy RODO, czyli unijnego ogólnego rozporządzenia o ochronie danych.

SPRAWDZAJ, CZY I JAK JEST DOPEŁNIANY OBOWIĄZEK INFORMACYJNY

Zawsze, gdy instalujemy aplikacje, do działania których niezbędne jest przetwarzanie danych osobowych, podmiot, który jest ich administratorem, powinien spełnić wobec nas obowiązek informacyjny. RODO zobowiązuje go, by dokonywał tego w sposób przejrzysty i zrozumiały, w zwięzłej formie, jasnym i prostym językiem. To bardzo ważne zwłaszcza wówczas, gdy podstawą zbierania i wykorzystywania danych jest nasza zgoda. Żeby uznać ją za prawidłową, musi być wyrażona dobrowolnie, a my musimy mieć świadomość, na co dokładnie się godzimy.

Warto pamiętać, że zgodnie z RODO powinniśmy zostać poinformowani o danych kontaktowych administratora, a także inspektora ochrony danych (o ile jest wyznaczony). Przepisy wymagają, byśmy otrzymali informacje o podstawie prawnej, na jakiej przetwarzane są nasze dane oraz o celach, dla których jest to robione czy o fakcie profilowania. Jeżeli nasze dane są przekazywane innym podmiotom, to również o tym musimy być poinformowani. Tak

samo jak o ich przesyłaniu do państw trzecich. RODO zobowiązuje też do informowania o tym, jak długo dane będą w określonym przypadku przetwarzane. Administrator musi poinformować nas również o naszych uprawieniach, takich jak prawo: dostępu do danych osobowych, sprostowania, usunięcia, ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych. A jeżeli przetwarzanie odbywa się na podstawie udzielonej zgody, to również o prawie do jej cofnięcia w dowolnym momencie. Powinniśmy również otrzymać informacje o prawie wniesienia skargi do organu nadzorczego, czyli Prezesa Urzędu Ochrony Danych Osobowych.

Zatem przy ściąganiu aplikacji warto zwrócić uwagę, jak ich twórcy i dostawcy wywiązują się z tego obowiązku, jak formułują klauzule zgód i polityki prywatności.

To tym bardziej istotne, że często instalacja aplikacji jest równoznaczna z akceptacją polityki prywatności, do treści której prowadzi osobny link. Nie każdy w niego klika, a gdy już to zrobi, to widząc dużo tekstu na ekranie małego telefonu, po prostu go nie czyta. To błąd. Można bowiem nieopatrznie wyrazić zgodę na coś, na co nie chcemy się godzić.

ZWRACAJ UWAGĘ, DO JAKICH DANYCH I FUNKCJI TELEFONU CHCE MIEĆ DOSTĘP APLIKACJA

Zanim zainstalujemy w swoim telefonie jakąkolwiek nową aplikację, warto dokładnie przeanalizować, do jakich danych i funkcji naszego urządzenia chcą mieć one dostęp. Przykładowo niektóre aplikacje domagają się dostępu do: informacji o naszej lokalizacji, zdjęć, kontaktów czy dokumentów. Warto zastanowić się, jaki jest cel takiego działania i wybierać te aplikacje, które najmniej ingerują w naszą prywatność.

Czasami dostęp do pewnych danych może być niezbędny do tego, by aplikacja spełniała swoją rolę. O ile to zrozumiałe, że np. mapy chcą mieć dostęp do naszej geolokalizacji (o czym więcej w kontekśccie ochrony danych osobowych w innych naszych materiałach https://giodo.gov.pl/pl/file/12481), o tyle dane te są zbędne w przypadku korzystania z gry czy aplikacji biurowej.

RODO duży nacisk kładzie na to, by administratorzy danych nie przetwarzali więcej danych niż jest to niezbędne dla osiągnięcia konkretnego celu (zasada minimalizacji danych). Aplikacja, z której korzystasz, nie powinna pozyskiwać więcej danych, niż te, które są niezbędne do jej prawidłowego działania.

PAMIĘTAJ, ŻE TYLKO ŚWIADOMA ZGODA JEST WAŻNA I POWINIENEŚ MÓC JĄ WYCOFAĆ W KAŻDEJ CHWILI

Za korzystanie z wielu „darmowych” aplikacji „płacimy” naszymi danymi, godząc się na ich wykorzystanie do różnych celów, najczęściej marketingowych. Na tej podstawie trafiają one niekiedy do wielu różnych podmiotów. Z tego też powodu na ekranie naszych urządzeń wyświetlają się nam spersonalizowane reklamy.

Zanim zainstalujemy aplikacje, warto więc sprawdzić, na co dokładnie się godzimy i czy swoją zgodę możemy wycofać równie łatwo, jak jej udzielaliśmy. Takie nasze prawo wynika bowiem wprost z RODO.

Co istotne, jeśli usługi społeczeństwa informacyjnego są oferowane bezpośrednio dziecku (gry, aplikacje edukacyjne, usługi streamingowe kierowane do dzieci), to do osiągnięcia przez nie 16 lat, zgodę na przetwarzanie ich danych musi wyrazić lub zaakceptować rodzic albo inna osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem. Warto podkreślić, że co do zasady RODO duży nacisk kładzie na ochronę dzieci, które nie zawsze mają świadomość swoich praw i zagrożeń związanych z prywatnością.

UWAŻAJ, BO APLIKACJE SŁUŻĄCE ROZRYWCE MOGĄ USZCZUPLIĆ TWOJE KONTO

Szczególną ostrożność warto zachować, korzystając z aplikacji służących rozrywce, jak np. gry i odtwarzacze filmów oraz muzyki. Nie zawsze, gdy gra jest darmowa, zdajemy sobie sprawę, że jej dodatkowe elementy, jak np. jej rozszerzenia, dodatkowe pojazdy w grach czy ich ulepszenia, lepsze uzbrojenie dla bohatera, są płatne. A jeśli gra jest połączona z numerem naszej karty kredytowej czy płatniczej, a my nieopatrznie z takich dodatków skorzystamy, to automatycznie obciążymy nasze konto nieplanowanymi, niechcianymi wydatkami.

Należy zwrócić uwagę, czy sklep z aplikacjami, z którego korzysta telefon, nie jest połączony z kartą płatniczą lub kredytową. Jeśli tak, wówczas należy bacznie zwracać uwagę na to, co instalujemy. Wybierając nieopatrznie płatne aplikacje, system, który je instaluje, uprzedzając nas o płatności, obciąży naszą kartę odpowiednią kwotą. Taka sytuacja często ma miejsce przy instalacji gier, których spora część jest płatna. Ponadto część z nich ma dostęp do naszej karty płatniczej połączonej ze sklepem i może wówczas ją obciążyć należnością za korzystanie z płatnych dodatków do gry. Gdy zdecydujemy się na takie zakupy, należy zwracać uwagę na warunki zakupu, w których często oferowane są opcje automatycznego odnawiania płatności, gdy wykorzystamy określony limit lub upłynie określony czas, bowiem skutkować to może systematycznym pobieraniem płatności za daną usługę bez naszej wiedzy, i to mimo iż z niej nie korzystamy.

Powinniśmy mieć też świadomość, że aplikacje służące rozrywce zbierają dane o tym, w co gramy, jakiej muzyki słuchamy czy jakie filmy oglądamy. Na tej podstawie tworzony jest nasz profil osobowy, wykorzystywany do wyświetlania spersonalizowanych reklam, mających na celu wzbudzenie w nas konkretnej potrzeby, a w efekcie zamówienie płatnych usług bądź kupno kolejnych produktów.

ZASTANÓW SIĘ, CZY INFORMACJIAMI O SWOICH OSIĄGNIĘCIACH SPORTOWYCH CHCESZ SIĘ DZIELIĆ ZE WSZYSTKIMI

Wakacje to okres wzmożonego użytkowania aplikacji sportowych. Te bardziej zaawansowane na podstawie sygnału GPS rejestrują nie tylko czas i przebytą trasę, ale są zintegrowane z zegarkami sportowymi, które mierzą tętno, wysokość, na jakiej się znajdujemy, gdzie i w jakim czasie odbywał się nasz trening. Zostały one zaprojektowane z myślą o sportowcach i

mierzeniu parametrów ich treningu, osiągnięć i tego, jak ich organizm reaguje podczas wysiłku. Ponieważ stały się powszechnie dostępne, również nam pomagają w analizie naszych sportowych wyczynów i ustaleniu programów pod cele sportowe, które chcemy osiągnąć.

Jeżeli nie zmienimy ustawień domyślnych tego typu aplikacji, w wielu przypadkach inni użytkownicy mogą na bieżąco śledzić nasze poczynania i ich wyniki. Taka funkcjonalność bywa niekiedy niebezpieczna, bo zdradza, gdzie w danym momencie jesteśmy.

Warto więc zastanowić się, jak bardzo chcemy pozbawiać się swojej prywatności. Czy po zakończonym treningu, wędrówce lub spływie kajakowym, chcemy w mediach społecznościowych dzielić się informacjami o tym, gdzie i kiedy trenowaliśmy, w jakim tempie biegliśmy lub płynęliśmy i jakie mieliśmy przy tym tętno. O ile dla znajomych taka informacja jest tylko ciekawostką, o tyle dla osoby o nieprzyjaznych zamiarach, np. złodzieja – jeśli nasze posty są dostępne dla wszystkich odwiedzających – to cenna informacja np. o tym, że nie ma nas w domu.

Poza tym na podstawie tego typu informacji można ustalić, jak często bywamy na basenie bądź w klubie fitness, a także pośrednio ustalić dane na temat naszego stanu zdrowia – co np. dla firm ubezpieczeniowych może być bardzo cenną informacją.

Świadome korzystanie z takich udogodnień jest bardzo ważne. Przestrogą może być głośne w ostatnim czasie zdarzenie polegające na tym, że żołnierze, którzy w mediach społecznościowych upublicznili dane ze swoich treningów biegowych, nieopatrznie ujawnili informacje o tajnych bazach wojskowych, na terenie których ćwiczyli. Jest to sytuacja nietypowa, jednak odzwierciedlająca, jak potencjalnie istotny wpływ nie tylko na nasze bezpieczeństwo może mieć publikacja takich informacji.

Wprawdzie zgodnie z RODO, nasza prywatność powinna być domyślnie, automatycznie, chroniona w najwyższym stopniu, jednak w praktyce bywa różnie. Warto więc dokładnie zapoznać się z ustawieniami domyślnymi tego typu aplikacji, byśmy wbrew naszej woli nie udostępnili zbyt dużo informacji na swój temat.

ŚWIADOMIE KORZYSTAJ ZE SMARTWATCHA, KTÓRY MOŻE WIEDZIEĆ WIĘCEJ NIŻ TELEFON

Coraz popularniejsze stają się smartwatche, czyli zegarki, które nie tylko pokazują godzinę, datę lub mają stoper. Są niemal jak miniaturowy smartphone. Pozwalają robić zdjęcia, odbierać rozmowy telefoniczne i komunikują się przy tym z naszym telefonem. W połączeniu z nim mogą być z jednej strony atrakcyjnym gadżetem, ale i źródłem bogatej wiedzy o nas i naszej aktywności.

Podobnie jak zegarki sportowe, niektóre smartwatche mogą mierzyć nasze kroki, a także tętno i to cały czas, niezależnie od tego, czy ćwiczymy, czy pracujemy, czy odpoczywamy. W ten sposób mogą gromadzić informacje o tym, jak aktywni jesteśmy w ciągu dnia, kiedy śpimy itp.

Warto mieć na uwadze to, że rejestrowane w tych urządzeniach dane o naszej aktywności mogą być niewłaściwie przetwarzane, np. przekazywane innym podmiotom, na co wskazał norweski urząd zajmujący się ochroną konsumentów. W jednym z raportów https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf zwrócił uwagę, ze niektórzy producenci smartwatch-y przetwarzali dane w chmurze, która znajdowała się w Chinach i nie gwarantowała odpowiedniego poziomu zabezpieczeń.

ZAREZERWUJ CZAS, BY PRZEJRZEĆ JUŻ ZAINSTALOWANE APLIKACJE

Biorąc pod uwagę, że w wakacje mamy nieco więcej czasu i nie jesteśmy tak zabiegani, jak w inne dni roku, warto przejrzeć także te aplikacje, które już zainstalowaliśmy lub są wgrane fabrycznie. Być może okaże się, że mają one dostęp do takich danych o nas, które wolimy chronić. Niekiedy może się okazać, że te dane są udostępniane wielu innym podmiotom, np. partnerom dostawcy usługi.

Poza tym często nie pamiętamy już informacji i ostrzeżeń związanych z aplikacjami, które instalowaliśmy kilka bądź kilkanaście miesięcy temu. Analiza ustawień może nam uświadomić, jak wiele danych o sobie zgodziliśmy się udostępniać, instalując aplikację lub nie modyfikując domyślnych ustawień.

Przegląd zainstalowanych aplikacji pod kątem ochrony naszej prywatności jest też o tyle istotny, że automatyczne aktualizacje wprowadzają nowe rozwiązania i nowe ustawienia, na które zazwyczaj nie zwracamy uwagi. Warto poświęcić czas, by być świadomym użytkownikiem tych rozwiązań.

NIE MOŻESZ MIEĆ PEWNOŚCI, ŻE TWÓRCA APLIKACJI ZAWSZE WŁAŚCIWIE POSTĘPUJE Z TWOIMI DANYMI

Użytkownicy telefonów komórkowych muszą mieć świadomość, że nie każda aplikacja, z której korzystają, działa zgodnie z przepisami dotyczącymi ochrony danych osobowych. Zdarzają się sytuacje, że pewne dane o nas są zbierane nadmiarowo albo producent oprogramowania ma dostęp do części zasobów naszego telefonu, o czym nas w ogóle nie informuje – choć powinien. Najczęściej takie informacje wychodzą na jaw przez przypadek. Coraz częściej media informują, że jakaś aplikacja w ukryty sposób nas szpieguje, wysyła zaszyfrowane pakiety danych itp. Warto więc śledzić medialne doniesienia, sprawdzać, czy sami u siebie nie zainstalowaliśmy takiego oprogramowania.

źródło:uodo.gov.pl

21-06-2018

- PDF

Wszystkie aktualności