Newsletter Ochrony Danych Osobowych - 6/2020

- Janusz Wyspiański (Inspektor Ochrony Danych Osobowych)

TEMAT: Wakacje od ochrony danych mogą Cię sporo kosztować. Bądź czujny!

……

Wakacje - dla wielu to czas zasłużonego relaksu i oderwania od codziennych spraw. Podczas gdy jedni korzystają z odpoczynku, niektórzy czekają na potknięcie tych pierwszych, wykorzystując wszelkie informacje pozwalające dokonać zuchwałych kradzieży. Kradzieży nie tylko dóbr materialnych, ale i tożsamości.

Przedstawiamy poniżej kilka rad, jak postępować i jak właściwie zadbać o swoje dane osobowe.

- **Nie zostawiaj dowodu w zastaw** - Nikt zgodnie z prawem nie może od nas wymagać, byśmy zostawili dokument tożsamości (np. dowód osobisty, paszport, prawo jazdy) w zastaw np. za wypożyczany sprzęt. Dokumenty są wydawane w celach ściśle określonych przepisami prawa i zawierają wskazany w nich katalog danych osobowych, który jest szerszy niż ten, jaki można uznać za niezbędny dla realizacji określonego celu.

  PRZYKŁAD!
  Kupując bilet na pociąg przez Internet, trzeba podać imię i nazwisko oraz informacje o dokumencie, który identyfikuje kupującego. Przewoźnik ma prawo do identyfikacji pasażera. Konduktor tylko w wyjątkowych sytuacjach np. podejrzewając, że bilet lub dokument tożsamości zostały sfałszowane, może zatrzymać bilet i dokument potwierdzający naszą tożsamość.

- **Nie pozwól robić kserokopii**

  Nie zgadzaj się na wykonywanie kserokopii dokument tożsamości. Sporządzenie kopii dowodów tożsamości jest legalne jedynie wtedy, kiedy wynika to wprost z przepisów rangi ustawy. Nawet gdy przedsiębiorca tłumaczy, że to jest wymagane do dochodzenia ewentualnych roszczeń, np. za zniszczony czy nieoddany sprzęt, nie zgadzaj się na to. Do tego wystarczające powinno być spisanie z dokumentu informacji, które będą pomocne przy dochodzeniu ewentualnych roszczeń, np. imienia i nazwiska czy numeru PESEL.

  Jeżeli przedsiębiorca postanowił spisać dane z dowodu osobistego, to domagaj się, by po tym, jak zwrócisz wypożyczony sprzęt, usunął je albo zwrócił ci formularz lub notatkę, na których je zapisał.

  PRZYKŁAD!
  Z podobnymi żądaniami o pozostawienie dokumentu albo pozwolenie na jego skopiowanie możemy się spotkać choćby w hotelowej recepcji. Nie wolno tego robić. Pracownik recepcji może jedynie poprosić nas o przedstawienie dokumentu w celu ustalenia naszej tożsamości. To oznacza, że recepcjonista ma prawo wglądu do naszego dowodu osobistego, ale nie do jego kopiowania czy zatrzymywania. W ostatnim czasie do UODO wpływają pytania dotyczące przetwarzania przez hotele danych osobowych swoich gości w postaci oświadczenia o przebytych chorobach, podróżach służbowych w związku z zapobieganiem rozprzestrzeniania się wirusa COVID. Hotele mogą przetwarzać dane dotyczące stanu zdrowia jedynie w sytuacji, gdy posiadają podstawę prawną dla takiego rodzaju działań.

  Nie publikuj zdjęć z wakacji, podczas Twojej nieobecności w domu.

  Podczas wakacji często chwalimy się fotografiami z odwiedzanych miejsc. Publikowanie zdjęć, świadczy o tym, że nie ma nas w domu. To nic innego jak zachęta dla potencjalnego złodzieja i zaproszenie do naszego domu. Jakiekolwiek zdjęcia, już po urlopie, udostępniaj ewentualnie tylko znajomym.
  Nie warto przechowywać plików zdjęciowych w pamięci dłużej niż to konieczne, nie tylko dlatego, że „zapychają pamięć urządzenia". Również dlatego, że w razie utraty lub sprzedaży urządzenia, mogą trafić w niepowołane ręce.

Nie dziel się danymi o swojej lokalizacji w mediach społecznościowych.

Niejednokrotnie już sceneria w tle zdradza, gdzie jesteśmy. Jednak na fotografii cyfrowej znajdziemy o wiele dokładniejsze dane dotyczące geolokalizacji, czyli informacji o położeniu geograficznym. Jedną z funkcji cyfrowych aparatów fotograficznych i smartfonów jest bowiem geotagowanie, dzięki któremu we właściwościach zdjęcia zapisywane są informacje o lokalizacji geograficznej aparatu. Na tej podstawie można ustalić dokładne położenie miejsca, w którym zdjęcie zostało wykonane.

Pamiętaj, że masz możliwość usuwania danych GPS, które określają lokalizację zrobionego przez Ciebie zdjęcia. W celu zwiększenia prywatności i bezpieczeństwa zaleca się usuwanie takich danych np. za pomocą mechanizmów wbudowanych w system Windows, jak również opcji dostępnych w ustawieniach aplikacji Aparatu. Media społecznościowe mają też funkcję ujawniania miejsca, w których właśnie przebywamy – lotniska, restauracje, muzea. Lepiej korzystać z nich z rozwagą.

Na urządzeniu korzystaj ze swojego połączenia z Internetem

A gdy musisz skorzystać z publicznej sieci Wi-Fi, to weź pod uwagę bezpieczne łączenie. Warto wyłączyć opcję automatycznego łączenia dla sieci publicznych, a przed skorzystaniem z sieci publicznej upewnij się, że łączysz się z odpowiednim punktem. Korzystaj z możliwości połączeń z siecią VPN, która stanowi bardzo ważne zabezpieczenie przed atakami hakerskimi.

Ponadto korzystaj jedynie z zabezpieczonych stron i pewnych źródeł. Ważnym sygnałem dla Ciebie będzie, że strona WWW, z której chcesz skorzystać jest „niezabezpieczona” lub połączenie jest „niezaufane”. Coraz częściej strony WWW korzystają z certyfikatu SSL (najłatwiej można rozpoznać to w adresie strony internetowej, gdy jej adres rozpoczyna się od „https://”, a nie od „http://”).

Zainstaluj na swoim urządzeniu oprogramowanie antywirusowe

Dzięki niemu możesz chronić swój sprzęt przed złośliwym oprogramowaniem, w tym wirusami, oprogramowaniem szpiegującym i ransomware. To bardzo ważne, w dobie powszechnego korzystania z Internetu, dokonywania płatności urządzeniami mobilnymi czy korzystania z bankowości elektronicznej.

<u>Ostrożnie udostępniaj nieznajomemu swój telefon</u>

„Przepraszam, rozładowała mi się bateria. Czy mogę zadzwonić z Pana/Pani telefonu?" Często użyczamy nasz telefon, a czemu nie?! Przecież chcemy pomóc, szybko, co złego może się stać? Niekiedy to oszuści chcący uzyskać dostęp do naszego urządzenia proszą o użyczenie Twojego telefonu. Czy tak samo udostępnilibyśmy nasz portfel? Zapominamy o tym, że nasz telefon komórkowy nie służy już „tylko" do komunikowania się. To jest nasze centrum dowodzenia, źródło informacji o nas. Mamy w nim zapisane daty urodzenia naszych członków rodziny, aplikacje bankowości elektronicznej, pocztę elektroniczną oraz wiele innych aplikacji pozwalających na ustalenie naszej tożsamości i stanu posiadania.

Chcesz pomóc, to poproś o nr telefonu, na który Ty sam wyślesz wiadomość do osoby, z którą ktoś inny chce się skontaktować i przekażesz jej informacje. Lepiej nie udostępniaj swojego telefonu nieznajomym.

Zabezpiecz się na wypadek kradzieży lub zgubienia telefonu

Przede wszystkim ustaw blokadę ekranu, co znacznie ograniczy ryzyko dostępu do Twoich danych. Warto również pomyśleć o włączeniu usługi lokalizującej urządzenie oraz umożliwiającej zdalne usuwanie zawartości telefonu lub jego blokadę. Wykonuj również regularnie kopie zapasowe danych, które znajdują się na Twoim urządzeniu, lub korzystaj z backupu w chmurze, dzięki czemu szybko odzyskasz dostęp do ważnych danych w przypadku awarii, zgubienia lub kradzieży telefonu.

Z poważaniem.
Janusz Wyspiański

ŹRÓDŁO DANYCH:

Strona internetowa UODO (uodo.gov.pl). https://uodo.gov.pl/pl/138/1575