LO semestr 2 Dn. 1.02.2021

SPOŁECZEŃSTWO W INTERNECIE

I. Cyfrowa tożsamość

Proszę obejrzeć:
https://www.youtube.com/watch?v=33kseZ4_FNs

Obecnie bardziej niż kiedykolwiek definiuje nas nasza cyfrowa tożsamość, dzięki wszechobecności mediów społecznościowych i tworzeniu wielu profili cyfrowych. Coraz więcej naszych działań online jest wykorzystywanych, aby nas kategoryzować, a także do określania ofert, usług i możliwości, które są nam przedstawiane.
Wraz z pojawieniem się przepisów takich jak RODO, organizacje zmuszone są uznać, że Dane osobowe (DO) są cennym towarem. Należy je nie tylko chronić, ale także zapewnić osobom fizycznym jasno określone prawa związane z ich tożsamością cyfrową.
Wraz z eksplozją usług w chmurze i elastycznych miejsc pracy znajdujemy się w sytuacji, w której nasza tożsamość jest przenośna, a jej granice elastyczne.

II. Trzy proste sposoby ochrony cyfrowej tożsamości

Utrata kontroli nad prywatnością w sieci jest zjawiskiem coraz bardziej powszechnym. Internet nie jest niczym więcej, niż wyciągnięciem ręki po błyskawiczną rezerwację hotelu, towary stale dostępne w sklepach online czy bezpłatne aplikacje. Stosowanie zasad zwiększających anonimowość internauty jest oceniane jako nużące, skomplikowane i czasochłonne. Fundacja Bezpieczniejwsieci.org przypomina o trzech prostych sposobach na zachowanie prywatności danych przy utrzymaniu komfortu użytkowania zasobów sieci.
Wystarczy zaadoptować 3 kroki, które w odczuwalny sposób uchronią naszą internetową tożsamość.

Wyłącz geolokalizację na swoim urządzeniu mobilnym

Pierwszy krok w jest prosty, wystarczy wziąć do ręki swój smartfon, tablet czy laptop i wyłączyć funkcję geolokalizacji. Wydaje się, że jest to mała rzecz, lecz geolokalizacja jest powodem największych nadużyć prywatności danych – GPS i WiFi pracują w każdym miejscu w którym pojawia sie użytkownik bez różnicy czy jest to kawiarnia czy centrum handlowe. Pozwala to dostosować reklamy do lokalizacji urządzenia – smartfon z aktywną lokalizacją i połączeniem z siecią wysyła raz na godzinę, dane do Google'a.

Wyłącz bezprzewodowy dostęp do sieci – korzystaj z niego jedynie w razie potrzeby

Użytkownik, któremu zależy na zachowaniu prywatności powinien wyłączyć stały dostęp smartfonów, tabletów czy laptopów do WiFi. Korzystanie z bezpłatnego bezprzewodowego Internetu jest akceptowalne pod warunkiem, że użytkownik sam

kontroluje i wybiera sieć, z którą chce się połączyć. Smartfony z włączoną funkcją WiFi stale poszukują punktu dostępu do sieci, dzieje się to bez wiedzy użytkownika. Urządzenie nie analizuje czy łączność z rozpoznaną siecią jest zgodna z prawem, bezpieczna itp. Ponadto smartfon z włączoną funkcją WiFi nadaje prawie nieustannie swój adres MAC, organizacje komercyjne zaczęły coraz poważniej interesować się tym unikalnym ID, ponieważ może być on używany jako cookie do śledzenia ruchu w sieci i profilu użytkownika w czasie rzeczywistym.

Wyloguj się po zakończeniu działania

Trzeci krok, wydaje się najtrudniejszy, lecz jego stosowanie wpływa wymiernie na ochronę danych osobowych. Ukończona praca na laptopie, sprawdzone konto w banku, aktualizacja na Facebooku – wszystkie te aktywności powinny kończyć się wylogowaniem. Jeśli użytkownik będzie bagatelizował daną czynność, w rzeczywistości "nie opuści" wirtualnego miejsca w którym przebywał. Wszystkie używane aplikacje, z których się nie wylogował są otwartymi drzwiami, przez które mogą wydostawać się prywatne dane. Zwiększa to ryzyko między innymi ataku clickjackingu czy śledzenia mediów społecznościowych. Aby lepiej chronić prywatność w sieci warto włączyć opcję przeglądarki, polegającą na czyszczeniu historii za każdym razem gdy jest ona zamykana.

Źródło: Fundacja Bezpieczniejwsieci.org

III. Jak dbasz o bezpieczeństwo swoich danych osobowych? Czy w ogóle o tym myślisz, korzystając codziennie z internetu? Czym w ogóle są dane osobowe?

Pojęcie danych osobowych to fundament, na którym opiera się prawo dotyczące ich ochrony. Ustawodawca dokonał podziału danych osobowych na zwykłe i szczególnie chronione (tzw. dane wrażliwe). Jak zabezpieczać te dane, aby nie wpadły w niepowołane ręce?

Dane wrażliwe

Dane wrażliwe (sensytywne) to wyodrębniona kategoria danych osobowych, które należy szczególnie chronić.

Akty prawne regulujące kwestie ochrony danych osobowych to przede wszystkim:

- Rozporządzenie o ochronie danych osobowych (RODO) – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;
- Ustawa z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości

Wymienione akty normatywne nie definiują wprost pojęcia danych wrażliwych, podają za to zamknięty katalog takich danych.

Zgodnie z nim, dane wrażliwe to informacje ujawniające m.in.:

- pochodzenie rasowe;
- pochodzenie etniczne;

- poglądy polityczne;
- przekonania religijne;
- światopogląd;
- przynależność do związków zawodowych;
- dane genetyczne (np. kod DNA, RNA);
- dane biometryczne (np. linie papilarne, kształt małżowiny usznej, odręczny podpis);
- dane dotyczące zdrowia;
- seksualność lub orientację seksualną.

Dla porównania, do danych osobowych zwykłych zaliczamy m.in. imię i nazwisko, adres zamieszkania, numer PESEL czy numer telefonu.

Dane wrażliwe

Ze względu na szczególny charakter danych wrażliwych ich przetwarzanie jest zabronione. Zakaz ten dotyczy zarówno przetwarzania w formie zautomatyzowanej, jak i niezautomatyzowanej. Przepisy prawa przewidują jednak pewne wyjątki od tej zasady.

Kiedy dopuszcza się przetwarzanie danych wrażliwych?

- Zezwalają na to przepisy prawa – np. ustawa o Straży Granicznej w sytuacjach zagrożenia bezpieczeństwa publicznego pozwala m.in. na pobranie osobom podejrzanym wymazów ze śluzówki policzków;
- jest to niezbędne dla ochrony życia, lub zdrowia, lub interesów osoby, której dane dotyczą, lub innej osoby – np. kontrola pandemii i jej rozprzestrzeniania się; obowiązek ratowania zdrowia lub życia ludzi; poza zakresem tej kategorii będą interesy ekonomiczne oraz majątkowe;
- dane takie zostały upublicznione przez osobę, której dotyczą – np. w prasie, w internecie; przy czym dane te muszą zostać podane do publicznej wiadomości w taki sposób, aby mogła się z nimi zapoznać bliżej nieokreślona liczba osób;
- osoba, której dane dotyczą, wyraziła pisemną zgodę na ich przetwarzanie – np. kandydat podczas procesu rekrutacji wyraził zgodę na przetwarzanie danych dotyczących jego stanu zdrowia;
- wykorzystanie tych danych jest niezbędne w celu dochodzenia praw przed sądem – np. zbadanie, czy doszło do prześladowania pracownika ze względu na jego pochodzenie etniczne.

Podmiot przetwarzający dane osobowe wrażliwe ma obowiązek prowadzenia rejestrów czynności przetwarzania danych.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

Art. 107. [Nielegalne przetwarzanie danych osobowych]

1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Źródło: *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych*, dostępny w internecie: sip.lex.pl [dostęp 8.12.2020 r.].

Ogólne zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych

O jakich zasadach należy pamiętać?

- Zasada czystego biurka – dokumenty z danymi wrażliwymi nie powinny znajdować się w ogólnodostępnym miejscu.

- W miejscu przetwarzania danych osobowych nie powinny przebywać osoby nieuprawnione.
- Pomieszczenie, w którym przetwarzane są dane osobowe powinno być zamykane na klucz.
- Komputery służące do przetwarzania danych powinny podlegać przeglądom antywirusowym.
- Należy pamiętać o szyfrowaniu danych.
- Powinno się regularnie zmieniać hasła dostępu.

Doszło do naruszenia bezpieczeństwa danych osobowych. I co teraz?

1. W ciągu 72 godzin od momentu stwierdzenia takiego naruszenia należy zawiadomić o nim Urząd Ochrony Danych Osobowych.
2. Administrator danych osobowych ma obowiązek bez zbędnej zwłoki zawiadomić o tym również osobę, której dane dotyczą.

Administratorem danych wrażliwych może być np.: przedsiębiorca lub pracodawca, który gromadzi takie dane w ramach prowadzonej przez siebie działalności, przychodnia lekarska, szpital, fundacja itp.

Słownik

administrator danych osobowych
podmiot publiczny lub prywatny, który decyduje o celach i sposobach przetwarzania danych osobowych; może być też wskazany w ustawie

dane biometryczne
dane osobowe dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiające lub potwierdzające jednoznaczną identyfikację tej osoby, w tym wizerunek twarzy lub dane daktyloskopijne

dane dotyczące zdrowia
dane osobowe dotyczące stanu zdrowia fizycznego lub psychicznego osoby fizycznej, w tym dane o korzystaniu z usług opieki zdrowotnej, które ujawniłyby informacje o stanie jej zdrowia

dane genetyczne
dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu, uzyskane przeważnie na podstawie analizy jej próbki biologicznej

przetwarzanie danych osobowych
wykonywanie różnego rodzaju operacji na danych osobowych, takich jak: przeglądanie, zbieranie, przechowywanie, przesyłanie, udostępnianie, zmienianie czy usuwanie

Źródło: https://epodreczniki.pl/a/przeczytaj/DNoDNE9hE