Jak być *zapomnianym* w internecie

Warszawa, 2020 r.

FUNDACJA bezpieczna cyberprzestrzeń

Urząd Komunikacji Elektronicznej | UKE

Spis treści

1. Wstęp....2
2. Ryzyka wynikające z braku zabezpieczenia prywatności w sieci....3
3. Informacje prawne....5
4. Jak zostać „zapomnianym" w internecie – praktyczne porady....8
   - 4.1 Mozilla Firefox – stacjonarne systemy operacyjne....9
   - 4.2 Mozilla Firefox – urządzenia mobilne....11
   - 4.3 Chrome – stacjonarne systemy operacyjne....12
   - 4.4 Chrome – urządzenia mobilne....14
   - 4.5 Microsoft Edge – stacjonarne systemy operacyjne....14
   - 4.6 Microsoft Edge – urządzenia mobilne....15
   - 4.7 Opera – stacjonarne systemy operacyjne....16
   - 4.8 Opera – urządzenia mobilne....17
   - 4.9 Safari – stacjonarne systemy operacyjne....18
   - 4.10 Safari – urządzenia mobilne....19
5. Usuwanie kont w najpopularniejszych portalach społecznościowych....20
   - 5.1 Facebook – urządzenia stacjonarne....20
   - 5.2 Facebook – urządzenia mobilne....22
   - 5.3 Twitter – urządzenia stacjonarne....23
   - 5.4 Twitter – urządzenia mobilne....24
6 Usuwanie konta w serwisach aukcyjnych....25
   - 6.1 Allegro – urządzenia stacjonarne....26
   - 6.2 Allegro – urządzenia mobilne....27
   - 6.3 OLX – urządzenia stacjonarne....27
   - 6.4 OLX – urządzenia mobilne....28

7 Usunięcie kont w usługach świadczonych przez Google....30
8 Usuwanie danych użytkownika z różnych for i sklepów internetowych, gier online i platform blogowych....32
9 Procedura zgłaszania do organu nadzorczego skargi na naruszenie ochrony danych osobowych....34
10 Nieskuteczne praktyki....36
11 Przydatne linki....37

1. Wstęp

W dobie rozwoju nowoczesnych technologii, zalewu informacji, a także popularności portali społecznościowych, jesteśmy szczególnie narażeni na utratę kontroli nad prywatnością. Nasza aktywność, zarówno zawodowa jak i osobista, coraz częściej rozgrywa się w internecie. W sieci budujemy i utrzymujemy więzi ze znajomymi oraz bliskimi, tam dzielimy się naszymi opiniami i robimy zakupy. Niestety, przeniesienie wielu obszarów codziennego życia do internetu może powodować, że prywatne informacje na nasz temat stają się publicznie dostępne. Często nie wiemy jak temu zapobiec i nie zawsze też zdajemy sobie sprawę, jakie ryzyko wiąże się z nieodpowiednim zabezpieczeniem naszych danych.

Prywatność w sieci to wyzwanie na tyle poważne, że potrzebę regulacji tego zagadnienia zauważono na gruncie prawa międzynarodowego, szczególnie w Unii Europejskiej. Prace nad rozwiązaniami prawnymi dotyczącymi kwestii prywatności w cyberprzestrzeni, a także liczne dyskusje na ten temat, zaowocowały wejściem w życie ważnego unijnego aktu - ogólnego rozporządzenia o ochronie danych (RODO).

W materiale przedstawiamy zbiór dobrych praktyk stanowiący wsparcie dla osób, które zgodnie z prawem chcą usunąć swoje dane z internetu. Pokazujemy też jakich czynności należy się wystrzegać i prezentujemy katalog tych działań które czasem stosowane są przez użytkowników internetu w celu usunięcia danych z sieci, w rzeczywistości są jednak nieskuteczne.

2. Ryzyka wynikające z braku zabezpieczenia prywatności w sieci

Podczas korzystania z sieci zostawiamy wiele cyfrowych śladów I nie zawsze mamy wpływ na to, jakie informacje o nas można odnaleźć w internecie. Mogą to być dane wpływające negatywnie na nasz wizerunek lub reputację. Zważywszy na znaczenie naszego uczestnictwa w życiu społecznym i zawodowym, jest to być może kluczowe ryzyko wynikające z braku zabezpieczenia prywatności.

Wielką popularnością wśród internautów cieszą się media społecznościowe. Dzielimy się tam ważnymi wydarzeniami z naszego życia, wyrażamy poglądy i opinie na temat istotnych dla nas zjawisk społecznych, obyczajowych, kulturalnych czy politycznych. Wszystkie te informacje pozwalają zbudować profil psychologiczny, definiujący nasze preferencje, a tym samym dający reklamodawcom wiedzę o tym, w jaki sposób dopasować do naszych potrzeb treści pojawiające się na odwiedzanych przez nas stronach.. Internetowa aktywność jest też ściśle powiązana z funkcjonowaniem algorytmów skrupulatnie analizujących sieciowe zwyczaje i zachowania. Zbierane informacje są przetwarzane w celu uzyskania większego obrazu społeczeństwa sieciowego i agregowane w postaci dużych, zmiennych i różnorodnych zbiorów danych (big data).

Warto też pamiętać, że publikując na portalach społecznościowych zdjęcia i filmy przedstawiające nas i naszych bliskich lub znajomych, potencjalnie zwiększamy ryzyko zaszkodzenia nam w wyniku zastosowania techniki deepfake, pozwalającej tak preparować

zdjęcia i nagrania, by w realistyczny sposób przedstawiały daną osobę w niekorzystnych, często kompromitujących sytuacjach. Materiały dostępne na profilach mogą posłużyć do niemal idealnego odtworzenia danej postaci w całkowicie nieprawdziwym środowisku. Technologia ta pozwala również na wkładanie w usta danej osoby wypowiedzi, które nigdy nie padły. Szczególnie narażone są na to osoby publiczne, których życie jest w sieci jest o wiele bardziej eksponowane. Spreparowane materiały mogą wyrządzić poważne szkody wizerunkowe, a także posłużyć do skutecznego manipulowania informacjami, które wpływać mogą na zachowania innych ludzi.

Aktywność w internecie zwiększa też ryzyko ataku hakerskiego. Przestępcy, korzystając z naszej nieuwagi, mogą przesłać nam np. spersonalizowaną wiadomość zawierającą złośliwego wirusa (tzw. spear phishing). Wówczas zagrożona jest nie tylko nasza prywatność, lecz także samo urządzenie oraz przechowywane w nim dane.
Niedostateczne zabezpieczenie prywatności w sieci wynika niekiedy z nieodpowiedniego korzystania z funkcjonalności samych urządzeń, np. z łączenia się z publicznymi, często niezabezpieczonymi sieciami wi-fi. Dotyczy to głównie naszych urządzeń mobilnych i jest coraz bardziej powszechne w dobie rosnącej popularności pracy zdalnej.

Niezabezpieczona prywatność to także ryzyko ustalenia lokalizacji danej osoby za pomocą analizy i agregacji danych związanych z aktywnością w internecie, zwłaszcza na portalach społecznościowych. Ryzyko tego typu jest tym większe, im częściej udostępniamy używanym przez nas aplikacjom dane geolokalizacyjne.

Niedoskonałe zabezpieczenie prywatności w internecie może również oznaczać, że informacje o nas (dane osobowe, dane kart kredytowych, zdjęcia, ale także dane służące do
uwierzytelnienia w systemach teleinformatycznych, w tym loginy i hasła) zostaną bez naszej zgody wystawione na sprzedaż. Tego typu informacje o internautach są najczęściej gromadzone w tzw. ukrytej sieci (deep web), która z uwagi na konieczność użycia specjalnego oprogramowania utrudniającego dostęp i na swój anonimowy charakter, jest polem działań niezgodnych z prawem, w tym transakcji pomiędzy przestępcami.

Udostępnienie naszych wrażliwych danych w sieci stwarza poważne ryzyko incydentów opartych na kradzieży tożsamości. Takie dane jak PESEL, adres zamieszkania czy informacje o karcie kredytowej, mogą umożliwić przestępcom osiągnięcie korzyści majątkowych.

3. Informacje prawne

Bycie „zapomnianym” czyli usunięcie z internetu łatwego i szybkiego dostępu do informacji o nas, daje nam możliwość ochrony naszych danych osobowych oraz wizerunku. Prawo do bycia „zapomnianym” w internecie wzbudziło zainteresowanie w związku ze sprawą obywatela Hiszpanii Mario Costeja Gonzaleza. Domagał się on od hiszpańskiego organu nadzorczego oraz hiszpańskiego oddziału Google usunięcia linków i innych odnośników do stron internetowych, na których znajdowały się jego dane osobowe (wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C 131/12 Google Spain). Była to na tyle istotna kwestia, że prawodawca postanowił zawrzeć w nowych regulacjach unijnych elementy dotyczące prawa do bycia „zapomnianym”.

Jakie mamy podstawy prawne do bycia „zapomnianym”?

Prawo do bycia „zapomnianym” to przede wszystkim prawo do usunięcia danych wtedy, kiedy przestają być potrzebne, albo kiedy ustaje podstawa, na której oparte było przetwarzanie tychże danych. Przesłanki pozwalające na skorzystanie z tego prawa przez osoby fizyczne reguluje art. 17 Rozporządzenia 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, zwanej powszechnie RODO (lub z jęz. angielskiego – GDPR). Prawo do bycia „zapomnianym” przysługuje, gdy:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
- dane osobowe były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

Rozporządzenie RODO we wszystkich państwach Unii Europejskiej stosowane jest bezpośrednio, co oznacza, że administratorzy danych osobowych mają wszędzie te same obowiązki, a osoby których dane są przetwarzane - te same prawa. Rozporządzenie stanowi, że jeżeli administrator upublicznił dane osobowe, to ma nie tylko obowiązek usunąć te dane ze swoich baz, ale także, biorąc pod uwagę dostępną technologię i koszt realizacji, podjąć działania mające na celu poinformowanie administratorów przetwarzających udostępnione przez niego dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych informacji lub ich replikacje. Istotnie wzmacnia to prawo do bycia „zapomnianym".

Do każdego przypadku korzystania z prawa do „zapomnienia" trzeba podchodzić indywidualnie i ze świadomością, że – niezależnie od trudności technicznych – prawo to nie zawsze będzie mogło być zastosowane:

- osoba fizyczna nie może usunąć wcześniej upublicznionych danych, jeśli naruszałoby to prawo innych osób do korzystania z wolności wypowiedzi lub prawa do informacji;
- organy publiczne i instytuty naukowe mogą przetwarzać nasze dane w celach archiwalnych, w celu prowadzenia badań naukowych i historycznych oraz w celach statystycznych;
- nasze dane mogą być przetwarzane również z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego.

Przepisy prawa pozwalają przetwarzać dane także w przypadku ustalenia, dochodzenia lub obrony roszczeń.
Prawo do bycia „zapomnianym" to jeden z najistotniejszych elementów obowiązujących obecnie przepisów dotyczących ochrony danych osobowych. Od początku spotykało się

ono ze zdecydowanym sprzeciwem wielu działających w internecie podmiotów wykorzystujących dane osobowe w celach reklamowych, ponieważ utrudnia im działania biznesowe. Niektórzy przeciwnicy prawa do bycia „zapomnianym" uważają też, że kłóci się ono z wolnością wypowiedzi. Kolejnym argumentem przeciwko temu rozwiązaniu była obawa, że będzie ono wykorzystywane przez osoby pragnące zataić dostępne publicznie informacje na przykład dotyczące ich niechlubnej przeszłości.

Mimo wszelkich tego typu obiekcji, prawo do bycia „zapomnianym" zostało zaimplementowane do europejskiego porządku prawnego i za brak jego przestrzegania administratorom grożą obecnie sankcje nakładane przez organ nadzorczy (Prezes Urzędu Ochrony Danych Osobowych) stojący na straży przestrzegania przepisów. Użytkownicy internetu otrzymali tym samym potężny oręż do wykorzystania w walce z administratorami, którzy bardzo niechętnie do tej pory usuwali dane ze swoich baz.

4. Jak zostać „zapomnianym” w internecie – praktyczne porady

Case study

Pan Kamil pracuje jako przedstawiciel handlowy i w ramach swoich obowiązków często podróżuje. W ostatnim czasie zauważył, że gdy przemieszcza się, dostaje wiele powiadomień dotyczących miejsca, w którym się znajduje, w tym także reklamy pobliskich restauracji i sklepów. Ilość treści wyświetlanych na telefonie Pana Kamila była uciążliwa i wzbudziła w nim wątpliwości co do ochrony jego prywatności.

Rozwiązanie: Pan Kamil powinien zmienić ustawienia prywatności w swojej aktualnej przeglądarce internetowej poprzez wyłączenie geolokalizacji.

Stopień naszej widoczności w sieci i to jak wiele danych na swój temat w niej zostawiamy, zależy w dużej mierze od ustawień komputera i od zastosowania programów, z których korzystamy. Dla przeciętnego użytkownika głównym łącznikiem z siecią jest przeglądarka stron internetowych. Korzystając z niej, często nieświadomie zostawiamy po sobie cyfrowe ślady – zarówno w sieci, jak i na używanym urządzeniu. Dane te są w różnoraki sposób wykorzystywane, o czym często nie mamy wystarczającej wiedzy, dlatego warto zwrócić większą uwagę na sposób ich przetwarzania.

Choć w internecie nigdy nie będziemy do końca anonimowi, warto zostawiać jak najmniej śladów cyfrowych.

By skuteczniej chronić prywatność, należy w pierwszej kolejności odpowiednio skonfi-

gurować swoją przeglądarkę. Dzięki korzystaniu z niej w trybie prywatnym udostępnimy mniej danych czy informacji dotyczących naszej aktywności online. Działanie to dotyczy historii przeglądania, wyszukiwania i tzw. ciasteczek (cookies).

Jak ustawić prywatne przeglądanie w najpopularniejszych przeglądarkach internetowych oraz w jaki sposób skonfigurować wybrane ustawienia prywatności?

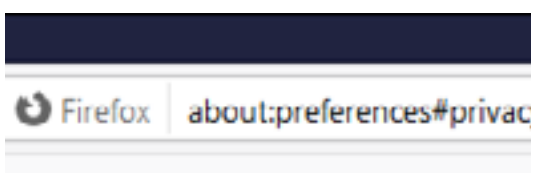
4.1 Mozilla Firefox – stacjonarne systemy operacyjne

Przeglądarka Firefox oferuje warianty ochrony w czterech obszarach:

- prywatności (różne poziomy ochrony przed śledzeniem, zarządzanie ciasteczkami, danymi logowania, hasłami, historia przeglądania, funkcje paska adresu);
- uprawnień (w kontekście geolokalizacji, kamery internetowej, mikrofonu, powiadomień i automatycznego odtwarzania materiałów audiowizualnych);
- danych zbieranych przez program Firefox;
- bezpieczeństwa (ochrona przed oszustwami i niebezpiecznym oprogramowaniem, zarządzanie certyfikatami).

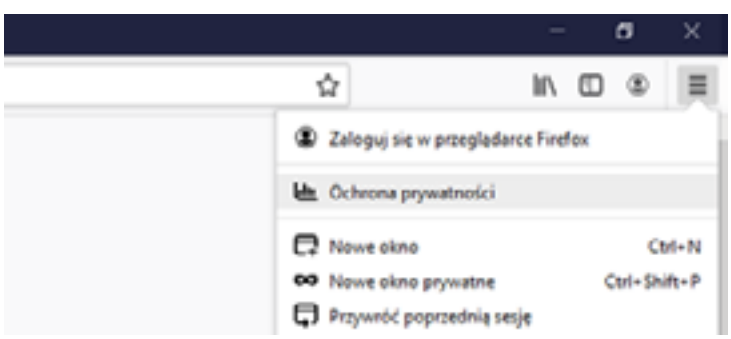
Instrukcja konfiguracji przeglądarki Firefox pod kątem obszaru prywatności[1]:

1. W pasku adresu wpisz „about:preferences#privacy” a następnie przejdź do strony (kliknij „enter”.)



Rysunek 1. Adres URL przeglądarki Firefox.

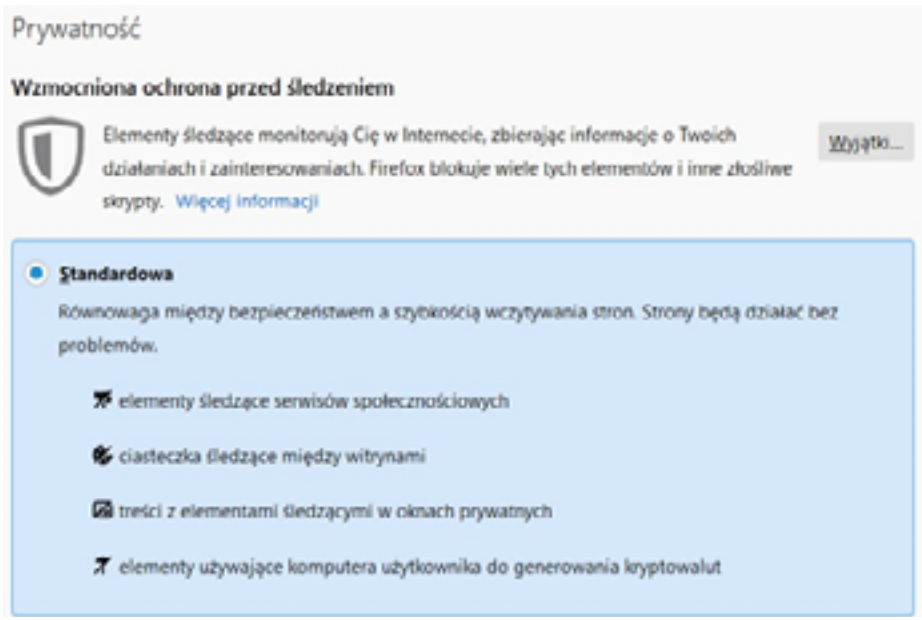
2. Możesz również wybrać „Ochronę prywatności” zaznaczając odpowiednią opcję w menu przeglądarki, zgodnie z poniższym zrzutem ekranu:



Rysunek 2. menu główne przeglądarki Firefox.

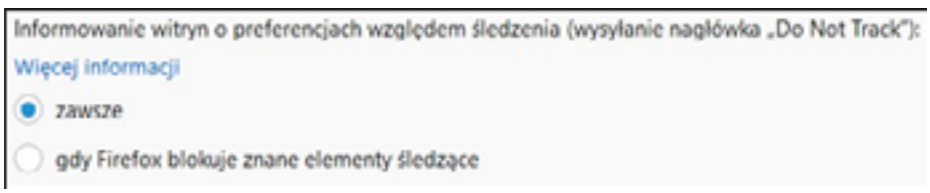
1 Dotyczy wersji: 70.0.1.

3. W sekcji „Wzmocniona ochrona przed śledzeniem” masz do wyboru 3 poziomy ochrony (standardowa, ścisła oraz własna). Każdemu użytkownikowi rekomendujemy wybranie poziomu ochrony „ścisłej”. Użytkownicy zaawansowani i bardziej świadomi zagrożeń mogą zdecydować się na „standardowy” poziom (ufając swojej wiedzy i stronom, które odwiedzają) lub sami wybrać, które elementy śledzące i skrypty powinny być blokowane („własna” konfiguracja). Domyślnie Firefox wybiera poziom „standardowy” czyli równowagę między bezpieczeństwem a szybkością wczytywania stron”. Blokowane są następujące elementy:



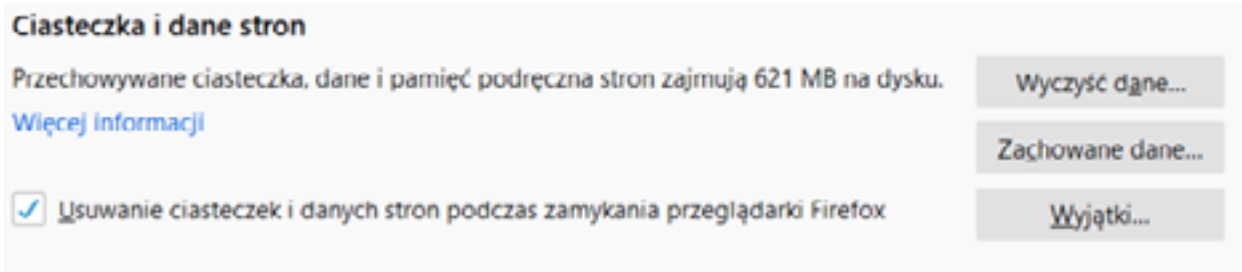
Rysunek 3. Menu prywatności w przeglądarce Firefox

4. W polu „Informowanie witryn o preferencjach względem śledzenia (wysyłanie nagłówka „Do Not Track”), zaznacz opcję „zawsze”, zgodnie z poniższym zrzutem ekranu:



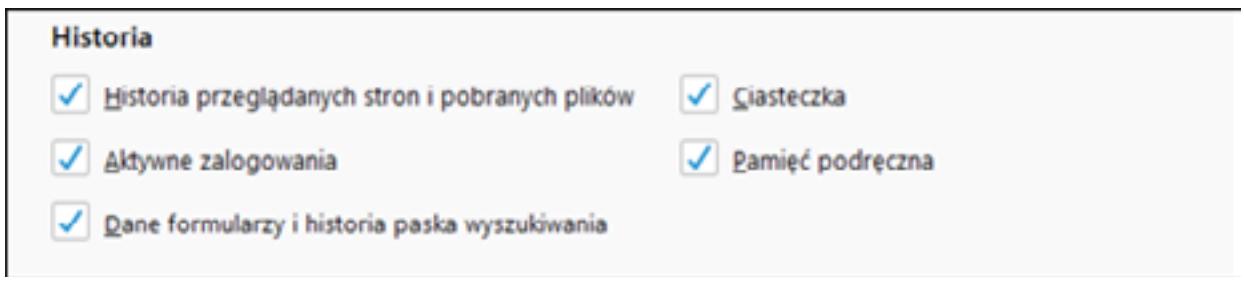
Rysunek 4. Preferencje śledzenia w przeglądarce Firefox

5. W sekcji „Ciasteczka i dane stron” możesz zaznaczyć opcję „Usuwanie ciasteczek i danych stron podczas zamykania przeglądarki Firefox”. Rekomendujemy zaznaczenie tej opcji. Możesz również podejrzeć zachowane przez przeglądarkę dane za pomocą przycisku „Zachowane dane”. Jeśli regularnie nie czyścisz przeglądarki pod kątem usuwania ciasteczek, w pamięci przeglądarki mogą znajdować się nawet setki megabajtów danych. Zaawansowani użytkownicy mają wybór – mogą zdecydować o tym, które serwisy mogą mieć specjalne uprawnienia w zakresie ciasteczek.



Rysunek 5. Opcje dotyczące ciasteczek i danych stron w przeglądarce Firefox

6. W sekcji „Historia” zwróć uwagę na możliwość permanentnego przeglądania w trybie prywatnym (w tym trybie przeglądarka nie zostawia śladów po aktywności użytkownika - hasła, pliki ciasteczek, historia). Przy okazji, pamiętaj, że tryb prywatny zawsze możesz włączyć stosując skrót klawiszowy **Ctrl+Shift+P**. Możesz też ustawić czyszczenie historii przeglądania za każdym razem, gdy zamykasz przeglądarkę. Warto rozważyć zaznaczenie następujących opcji:

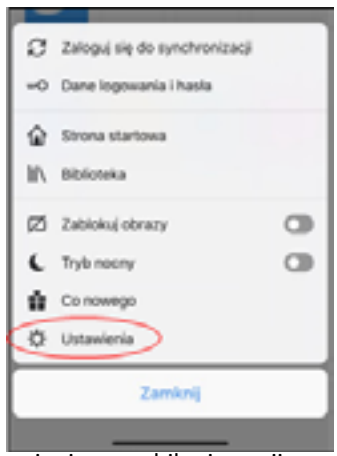


Rysunek 6. Opcje historii przeglądania w przeglądarce Firefox

4.2 Mozilla Firefox – urządzenia mobilne

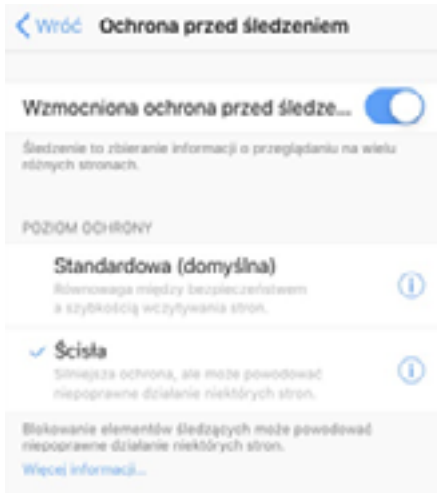
Ochrona przed śledzeniem jest również dostępna z poziomu urządzeń mobilnych[2]. Konfigurację prywatności można dokonać poprzez wykonanie następujących kroków, niemal analogicznie do wersji na stacjonarnej:

1. Uruchom przycisk „menu” w prawym dolnym rogu uruchomionej przeglądarki.
2. W menu głównym wybierz opcję „Ustawienia”:



Rysunek 7. Ustawienia w mobilnej wersji przeglądarki Firefox

3. Wybierz i zmień konfigurację prywatności w sekcjach „Dane logowania i hasła”, „Ochrona przed śledzeniem” oraz „Zarządzanie danymi”, zgodnie z Twoimi preferencjami. Poniżej przykładowe ustawienia, z których możesz skorzystać. Pamiętaj, że możesz użyć takich samych ustawień na jak swoim komputerze.



Rysunek 8. Ochrona przed śledzeniem w mobilnej wersji przeglądarki Firefox

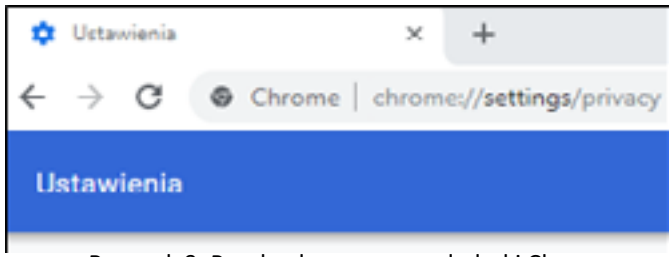
4. Wersja mobilna Firefoxa umożliwia również przejście w tryb prywatny. Na stronie startowej przyciśnij ikonkę obok menu. Następnie wybierz tryb prywatny w nowo otwartej karcie (ikona w lewym dolnym rogu aplikacji).

4.3 Chrome – stacjonarne systemy operacyjne

Przeglądarka Chrome może być skonfigurowana pod kątem efektywniejszego zarządzania prywatnością. Użytkownik wykonuje te czynności z poziomu „ustawień”. Funkcje powiązane z bezpieczeństwem znajdują się również w sekcji „autouzupełnianie”.

Instrukcja konfiguracji przeglądarki Chrome pod kątem wzmocnienia prywatności i bezpieczeństwa użytkownika:

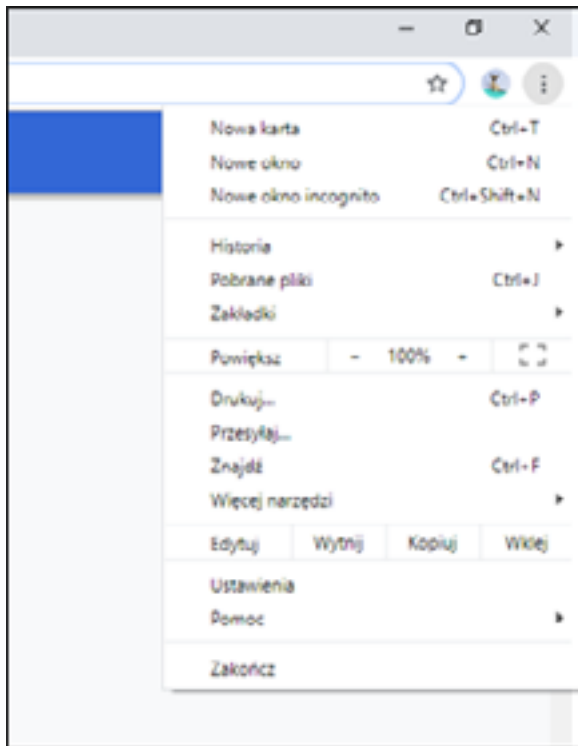
1. Po uruchomieniu Chrome, w pasku adresowym wpisz „chrome://settings/privacy”:



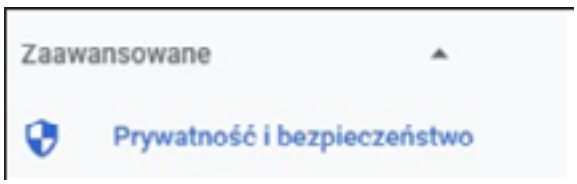
Rysunek 9. Pasek adresowy przeglądarki Chrome.

2. Możesz też po uruchomieniu przeglądarki Chrome w prawym górnym rogu ekranu

uruchomić menu i przejść do ustawień, a dalej „Prywatność i bezpieczeństwo”:



Rysunek 10. Menu główne w przeglądarce Chrome.



Rysunek 11. Przycisk Prywatność i bezpieczeństwo w przeglądarce Chrome.

3. W sekcji „Prywatność i bezpieczeństwo” rekomendujemy włączenie funkcji <Wysyłaj żądanie „Bez śledzenia” podczas przeglądania>. Pamiętaj jednak o tym, że nie wszystkie witryny będą stosować się do tego żądania i część witryn będzie nadal gromadzić pewne informacje.
4. Możesz wyczyścić dane przeglądania, w tym ciasteczka. Warto tu zwrócić uwagę na zaawansowane ustawienia, które umożliwią nam wyczyszczenie danych przeglądania (w tym haseł zapamiętanych w witrynach oraz danych udostępnianym aplikacjom). Co pewien czas (np. raz w miesiącu) warto czyścić dane przeglądania, daje nam to większą kontrolę nad danymi, które przekazujemy do sieci.
Funkcję „Ładuj wstępnie strony, by przyspieszyć przeglądanie i wyszukiwanie” możesz odznaczyć. Tego typu optymalizacja nie da ci zauważalnej korzyści i komfortu w przeglądaniu stron. Przyczynia się za to zbierania większej ilości informacji o twoich preferencjach.
5. Chrome umożliwia przejście w tryb prywatny. W tym trybie, jak zapewnia producent, przeglądarka nie zapisuje historii przeglądania, plików cookie, danych stron ani

informacji podanych w formularzach. Aktywność użytkownika jest jednak nadal widoczna dla stron internetowych, które użytkownik odwiedza. Tryb incognito uruchomisz za pomocą skrótu klawiszowego **Ctrl+Shift+N**.

4.4 Chrome – urządzenia mobilne

Funkcje dotyczące prywatności i bezpieczeństwa znajdziesz też w wersji Chrome (usługa „Google") na urządzenia mobilne. Konfigurację prywatności zalecamy jednak wykonać w wersji stacjonarnej, poprzez użycie funkcji synchronizacji (zobacz panel „Ustawienia" w Twojej przeglądarce). W samej aplikacji zalecamy zapoznanie się jednak z funkcją „Prywatność", którą można uruchomić
z poziomu głównego menu naciskając ikonę w prawnym dolnym rogu urządzenia4.

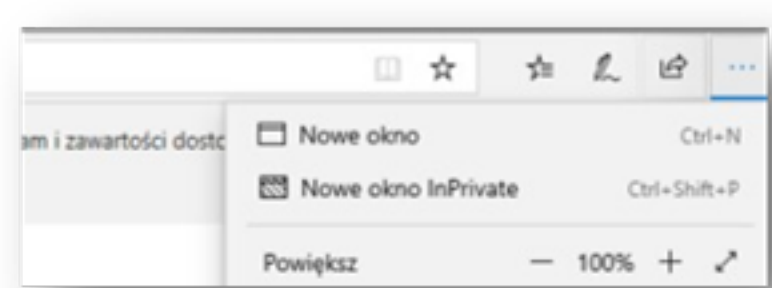
Z poziomu aplikacji mobilnej można m.in. usunąć historię przeglądania oraz zezwolić witrynom na sprawdzanie czy użytkownik ma zapisane formy płatności.

4.5 Microsoft Edge – stacjonarne systemy operacyjne

Najnowsza wersja przeglądarki Microsoftu pozwala nam na skorzystanie z trybu InPrivate, który w swoich założeniach ma na celu wykluczenie przechowywania czegokolwiek na twardym dysku użytkownika (historia, tymczasowe pliki internetowe i pliki cookie).

By uruchomić tryb InPrivate zgodnie ze wskazówkami producenta należy wykonać następujące kroki:

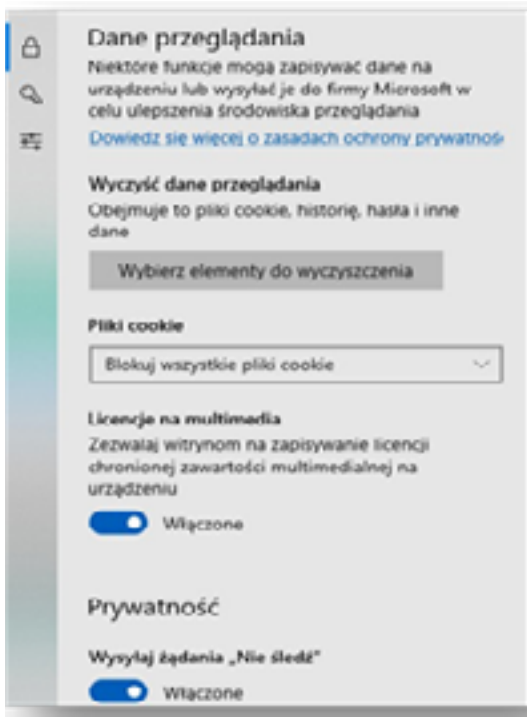
1. Kliknij przycisk „Ustawienia i nie tylko" w prawym górnym rogu przeglądarki. Możesz użyć skrótu klawiszowego Ctrl + X. Menu wygląda następująco:



Rysunek 12. Menu główne przeglądarki Microsoft Edge.

2. Wybierz z listy rozwijanej „Nowe okno InPrivate" lub wykorzystaj skrót klawiszowy Ctrl+Shift+P.

Nie zapominaj o pozostałych funkcjach przeglądarki, które dotyczą prywatności oraz twojego bezpieczeństwa! Dedykowana sekcja znajduje się w „Ustawieniach” po przejściu z menu „Ustawienia i nie tylko”. Dostępne są następujące funkcje, zgodnie ze zrzutem, w którym przedstawiamy fragment przykładowej konfiguracji. Zauważ, że polecamy m.in. blokowanie wszystkich plików cookie oraz wysyłania żądania „Nie śledź”.

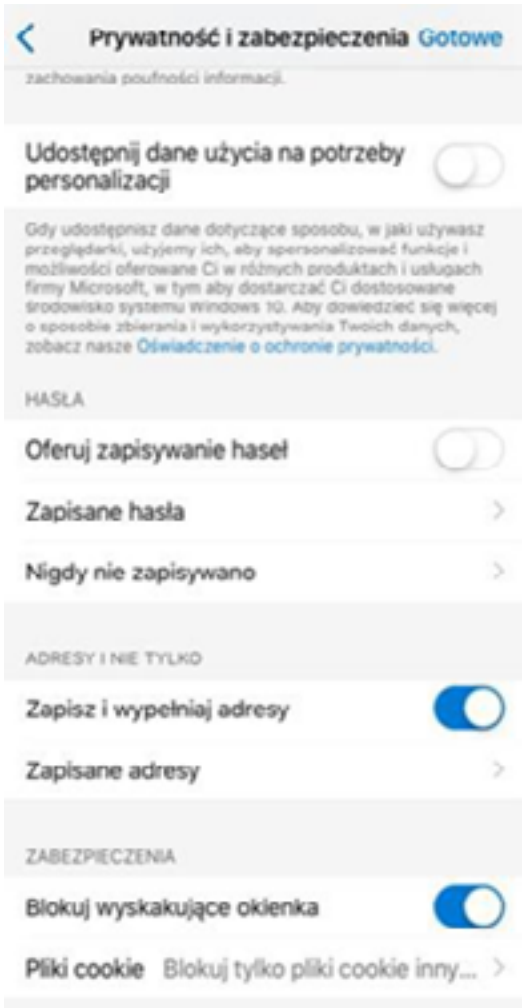


Rysunek 13. Opcje prywatności w przeglądarce Microsoft Edge.

4.6 Microsoft Edge – urządzenia mobilne

Te same opcje w zakresie prywatności są dostępne na urządzeniu mobilnym. Aby do nich dotrzeć skorzystaj z naszej instrukcji:

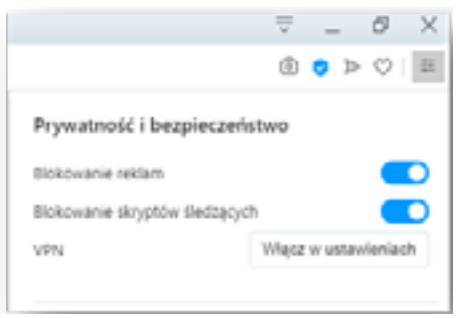
1. Otwórz aplikację na swoim urządzeniu mobilnym.
2. Przejdź w „Ustawienia” poprzez kliknięcie w główne menu (prawy dolny róg aplikacji).
3. Pierwsze na liście znajdują się „Prywatność i zabezpieczenia” - użyj tej opcji, by skonfigurować swoją przeglądarkę pod kątem danych, którymi dzielisz się z siecią w czasie przeglądania internetu. Zgodnie z poniższym zrzutem, opcje są analogiczne do wersji stacjonarnej:



Rysunek 14. Opcje prywatności w przeglądarce Microsoft Edge.

4.7 Opera – stacjonarne systemy operacyjne

Podstawowa konfiguracja przeglądarki Opera pod kątem prywatności może być wykonana przy użyciu panelu bocznego, który aktywuje się po wciśnięciu przycisku „Łatwa konfiguracja” (prawy górny róg ekranu). Użytkownik powinien otrzymać możliwość zmian w zakresie blokowania reklam i śledzących skryptów, a także może włączyć wbudowany tryb VPN („Virtual Private Network”) umożliwiający ochronę naszego ruchu sieciowego w warstwie aplikacji Opera. Poniżej nasza konfiguracja na zrzucie ekranu:

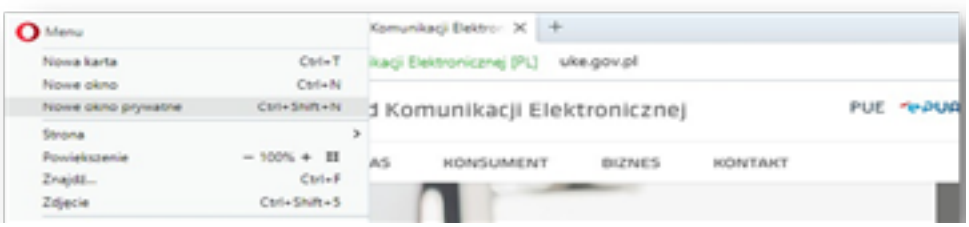


Rysunek 15. Opcje prywatności w przeglądarce Opera.

Jak łatwo można zauważyć, Opera oferuje również funkcję czyszczenia przeglądarki. Co tam znajdziemy? Już w wersji „podstawowej” usuniemy całą historię przeglądania, ciasteczka, dane witryn oraz obrazy i pliki w pamięci podręcznej. Jak w każdej innej przeglądarki znajdziemy też zakres czasu, który nas interesuje.

W przypadku przeglądarki Opera, by włączyć tryb zapewniający większą prywatność, użytkownik powinien po
uruchomieniu przeglądarki wybrać z menu głównego opcję „Nowe okno prywatne”.
Jak zapewnia producent, po zamknięciu okna prywatnego Opera usunie dane takie jak historia przeglądania, elementy pamięci podręcznej (cache) i ciasteczka.

Możesz również rozpocząć prywatny tryb przeglądania poprzez wciśnięcie klawiszy **Ctrl+Shift+N**.



Rysunek 16. Ilustracja pomocnicza wyjaśniająca jak włączyć tryb prywatny w przeglądarce Opera.

4.8 Opera – urządzenia mobilne

Testowana przez nas mobilna wersja Opery (aplikacja „Opera Touch”) posiada identyczne funkcje w zakresie prywatności. Na uwagę zasługuje jednak ta, która chroni nas przed potencjalnym zagrożeniem w postaci oprogramowania kopiącego kryptowaluty. Poniżej zrzut ekranu dotyczący naszej przykładowej konfiguracji:

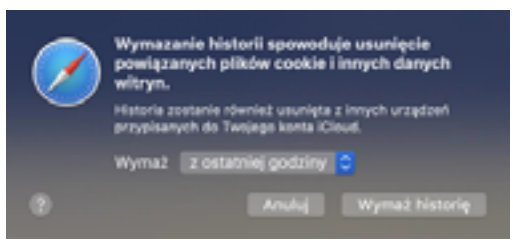
Rysunek 17. Opcje prywatności w przeglądarce Opera.

4.9 Safari – stacjonarne systemy operacyjne

Użytkownicy urządzeń firmy Apple opartych na systemach operacyjnych iOS (komputery Mac, smartfony iPhone) korzystają najczęściej z przeglądarki Safari, którą także można skonfigurować pod kątem prywatności. Zgodnie z instrukcją producenta, za wszystko odpowiada panel „Prywatność", który reguluje ustawienia usuwania i blokowania danych wykorzystywanych przez witryny. Upewnij się, że poniższe opcje są zaznaczone:

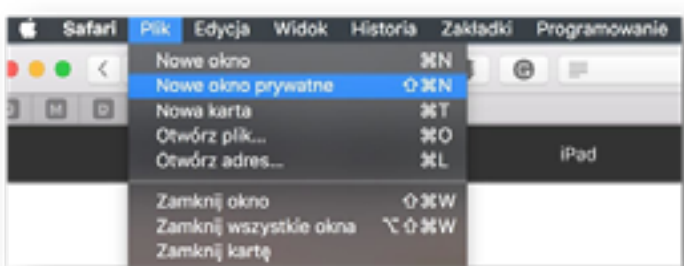
□ Zapobiegaj śledzeniu poza witryną
□ Blokuj wszystkie cookie

Co do usuwania historii odwiedzania stron w Safari – jest ono bardzo proste. Wystarczy w aplikacji Safari użyć w ramach menu „Historia" opcji „Wymaż historię". Usunięcie historii jest kompletne i dotyczy wszelkich danych, zgodnie z poniższym zrzutem:



Rysunek 18. Historia przeglądania w przeglądarce Safari.

Safari oferuje prywatny tryb przeglądania, a także możliwość ustawienia tego trybu jako domyślny (za każdym razem gdy uruchamiamy przeglądarkę). Aby tego dokonać należy po włączeniu przeglądarki w poleceniu „Plik" z listy rozwijanej wybrać opcję „Nowe okno prywatne". W celu włączenia tego trybu na stałe należy w poleceniu „Preferencje" wybrać przycisk „Ogólne", w dalszej kolejności, po otworzeniu Safari - „Wyświetla", a następnie „Nowe okno prywatne".

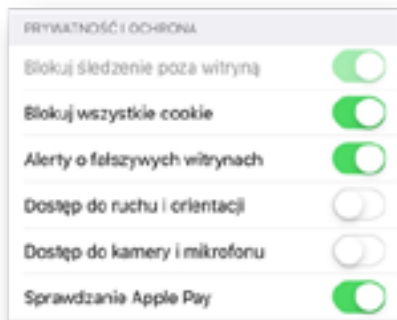


Rysunek 19. Ilustracja pomocnicza wyjaśniająca jak włączyć tryb prywatny w przeglądarce Safari.

Tryb prywatny przeglądarki Safari zapewnia m.in. izolację przetwarzanych informacji na każdej z otwartych kart trybu prywatnego, brak zapamiętywania adresów odwiedzanych stron, brak zapamiętywania zmian w plikach cookie oraz zapobieganie śledzenia na witrynach internetowych (dotyczy niektórych witryn). Pełen zakres usług trybu prywatnego dostępny jest na stronie wsparcia producenta w „Podręczniku użytkownika Safari".

4.10 Safari – urządzenia mobilne

Safari oferuje te same opcje dotyczące prywatności także w aplikacji mobilnej dedykowanej iPhonom. Na ekranie głównym smartfona należy wybrać „Ustawienia", a następnie znaleźć na liście aplikację Safari. Po przejściu do dodatkowego menu trzeba zaznaczyć wybrane opcje w sekcji „Prywatność i ochrona", zgodnie z przykładem na zrzucie ekranu:



Rysunek 20. Prywatność i Ochrona w przeglądarce Safari.

W mobilnym Safari również korzystać można z trybu prywatnego. W tym celu należy wejść w aplikację, a następnie dotknąć ikony w prawym dolnym rogu. By rozpocząć surfowanie w bezpieczniejszym trybie należy wybrać opcję „Prywatne".

5. Usuwanie kont w najpopularniejszych portalach społecznościowych

5.1 Facebook – urządzenia stacjonarne

Case study

Pani Joanna podejmuje pracę w wymarzonym zawodzie. Nowy pracodawca podchodzi jednak bardzo rygorystycznie do kwestii wizerunku pracowników w sieci. Korzystanie z portali społecznościowych, w tym Facebooka i Twittera, w jej przypadku nie wchodzi w grę.

Rozwiązanie: Pani Joanna musi na stałe usunąć swoje konto na Facebooku oraz Twitterze. Nie wystarczy tylko dezaktywacja konta.

Facebook jest jednym z najpopularniejszych portali społecznościowych - na świecie i w Polsce. Skuteczne „zapomnienie" w obszarze tego serwisu nie jest jednak zadaniem łatwym. Powinniśmy zacząć od tego, że użytkownik może nie tylko konto usunąć, ale także dezaktywować. Należy być świadomym, że sama dezaktywacja konta na Facebooku jest jedynie jego zawieszeniem z możliwością powrotnej aktywacji w dowolnym czasie, a sam Facebook zapisze dane użytkownika w swoich archiwach, właśnie po to, by móc na żądanie użytkownika je przywrócić.

Zawieszenie (dezaktywacja) konta na Facebooku - krok po kroku:

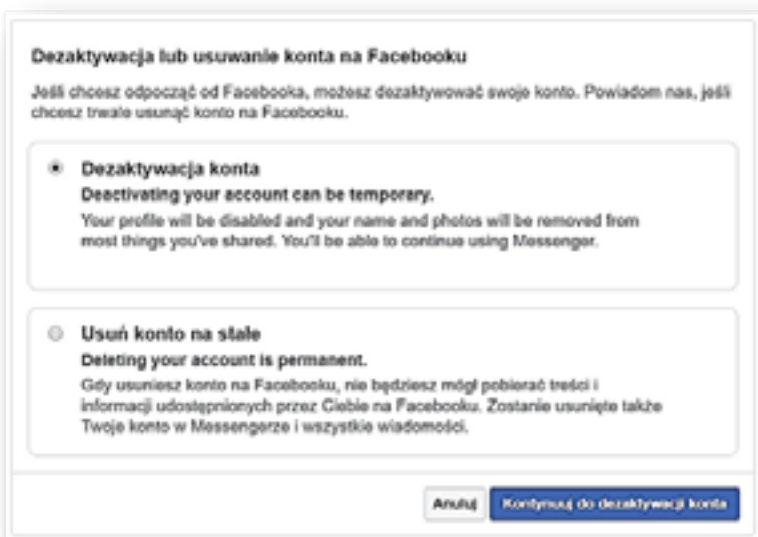
1. zaloguj się na swoje konto;
2. z rozwijanej listy (prawy, górny róg, obok ikony ze znakiem zapytania) wybierz „Ustawienia”;
3. po lewej stronie ekranu pojawią się opcje i w „Ustawieniach ogólnych” użytkownik powinien wybrać opcję „Twoje informacje na Facebooku”;
4. kliknij w przycisk „Dezaktywacja lub usunięcie konta na Facebooku” i postępuje zgodnie z informacjami na ekranie.

Można również rozpocząć procedurę dezaktywacji konta poprzez aktywację niniejszego linku.

Dezaktywacja konta spowoduje wyłączenie profilu użytkownika oraz usunięcie imienia, nazwiska i zdjęć z większości materiałów jakie użytkownik udostępniał na Facebooku. Uwaga: pewne dane mogą pozostać nadal widoczne dla innych osób, na przykład imię i nazwisko na listach znajomych i wszelkie dane w wysłanych wiadomościach. Przywrócenie konta polega na zwykłym zalogowaniu się do niego za pomocą danych uwierzytelniających, czyli adresu e-mail i hasła użytkownika.

Usunięcie konta na Facebooku krok po kroku:

1. zaloguj się na swoje konto;
2. wybierz opcję usunięcia konta na Facebooku korzystając z przeglądarki internetowej. Powinno ukazać się poniższe okno:



Rysunek 21. Dezaktywacja lub usuwanie konta na Facebooku. Źródło: Facebook.com

3. po potwierdzeniu chęci usunięcia konta musisz zatwierdzić decyzję hasłem i przepisaniem kodu captcha oraz ponownie potwierdzić usunięcie konta.

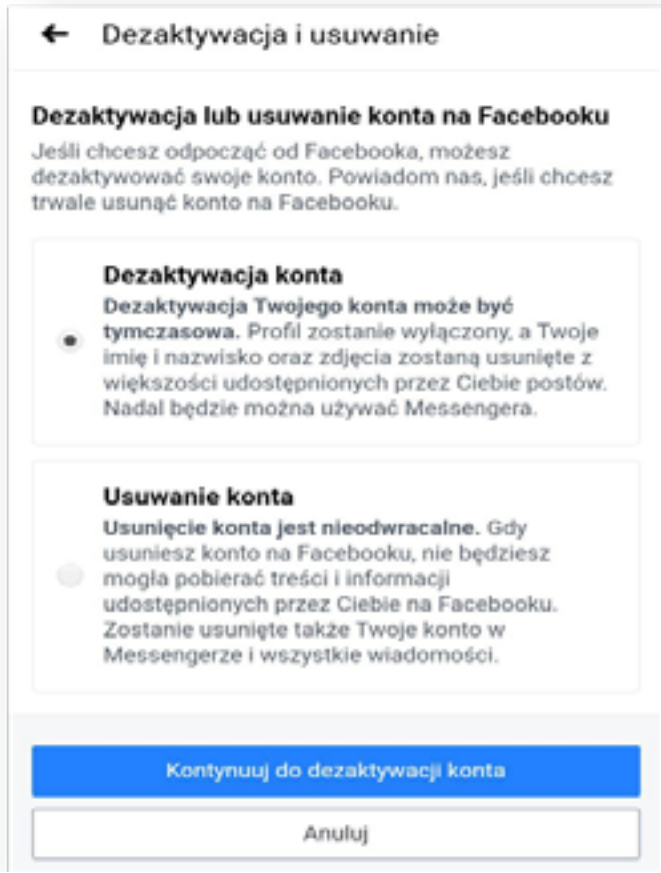
Uwaga: wykonanie tych wszystkich czynności wciąż nie powoduje natychmiastowego usunięcia konta. Użytkownik otrzymuje jeszcze okres próbny, podczas którego otrzyma na swój adres e-mail wiadomości przypominające o tym, że dane konto jest usuwane i jeśli zdecydujemy się zalogować na nie w tym czasie, proces usuwania konta zostanie przerwany. Nie będą także widoczne żadne udostępnione wcześniej przez użytkownika treści. Jedynie wysyłane przez niego wiadomości wciąż będą znajdować się u ich odbiorców. Opublikowane przez użytkownika materiały są dość długo usuwane z serwerów Facebooka. Może zająć to nawet 90 dni! Ten proces jest niezależny od faktu, że nasze dane nie będą już widoczne w witrynie portalu społecznościowego.

5.2 Facebook - urządzenia mobilne

Usunięcie na zawsze naszego konta na najpopularniejszym portalu społecznościowym jest również możliwe poprzez aplikację mobilną. Instrukcja jest niemal identyczna jak w przypadku wersji webowej (z której najprawdopodobniej korzystasz na komputerze). Szczegółowe informacje krok po kroku dostępne są w Centrum Pomocy Facebooka.

Zapoznaj się z sekcją „Jak trwale usunąć konto?”. Masz do wyboru następujące opcje:

Rysunek 22. Usunięcie konta Facebook na urządzeniu mobilnym. Źródło: Facebook.com



Rysunek 23. Dezaktywacja i usunięcie konta na mobilnej aplikacji Facebooka.

5.3 Twitter – urządzenia stacjonarne

Usunięcie konta na Twitterze jest znacznie prostsze niż na Facebooku. Portal nie dzieli także usługi na dezaktywację i usunięcie.

Usunięcie twitterowego konta krok po kroku:

1. zaloguj się na swoim koncie poprzez stronę główną Twittera;
2. w panelu po lewej stronie, po kliknięciu w przycisk „Więcej”, odnajdziesz rozwijaną listę;
3. kliknij w „Ustawienia i prywatność”, a następnie „Konto” - na samym dole pojawi się możliwość dezaktywacji konta. Przeczytaj uważnie informacje, które pojawią się w ramce.

Rysunek 24. Ilustracja pomocnicza wskazująca gdzie znajduje się przycisk dezaktywacji (usunięcia) konta.

Użytkownik powinien potwierdzić dezaktywację konta i podać swoje hasło. Po dezaktywacji proces całkowitego usunięcia konta i wpisów z serwerów trwa 30 dni.

5.4 Twitter – urządzenia mobilne

Taka sama procedura dezaktywacji konta jest dostępna w aplikacji mobilnej. Aby wejść w główne menu aplikacji, kliknij na swój awatar (lewy górny rok ekranu), a następie postępuj według analogicznych instrukcji jak w wersji stacjonarnej.

6. Usuwanie konta w serwisach aukcyjnych

Case study

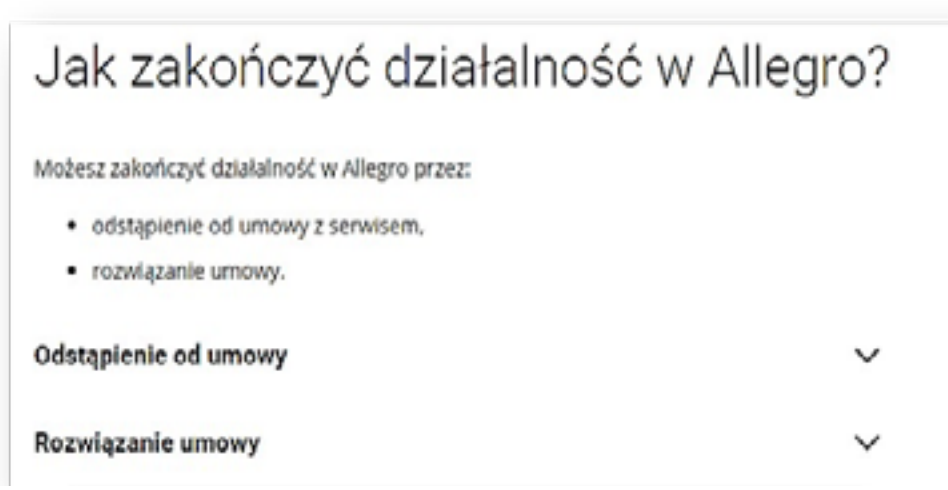
Pani Edyta prowadzi sprzedaż odzieży na Allegro. Wspólnie z zespołem zdecydowała rozszerzyć działalność o sprzedaż na rynku międzynarodowym i dlatego utworzyła konto także w innym serwisie aukcyjnym, umożliwiającym sprzedaż za granicą. Od kilku miesięcy sprzedaż poprzez międzynarodowy serwis aukcyjny zaczęła przynosić znaczne przychody. Pani Edyta zdecydowała, że skupi się wyłącznie na sprzedaży zagranicznej i tym samym zrezygnuje z prowadzenia konta aukcyjnego na Allegro.

Rozwiązanie: Pani Edyta powinna wypełnić formularz dostępny na stronie Allegro w celu rozwiązania umowy.

Tysiące Polaków korzystają każdego dnia z serwisów aukcyjnych. Portale te często kuszą nas konkurencyjnymi cenami, a ponadto są intuicyjne i proste w nawigacji. Analiza naszej aktywności w serwisach aukcyjnych mówi wiele o naszych preferencjach zakupowych, przyzwyczajeniach czy hobby – nie zawsze za nasza wiedzą i zgodą. Również w tego typu serwisach mamy prawo usunąć swoje dane. Użytkownik musi jednak pamiętać, że w związku z przepisami szczególnymi, pewne jego dane muszą być w tego typu serwisach nadal przetwarzane, przez czas, który określa artykuł 118 kodeksu cywilnego.

6.1 Allegro – urządzenia stacjonarne

Użytkownik może usunąć swoje dane osobowe z Allegro. Musi jednak najpierw rozwiązać swoją umowę z serwisem poprzez wysłanie stosownego wniosku. Odpowiednie hiperłącze można także odnaleźć dzięki użyciu przeglądarki po wpisaniu hasła „rozwiązanie umowy z Allegro". Powinniśmy odszukać witrynę z następującym pytaniem:



Rysunek 25. Odstąpienie od umowy z Allegro.

Użytkownik przed podjęciem się wypowiedzenia umowy z Allegro powinien:

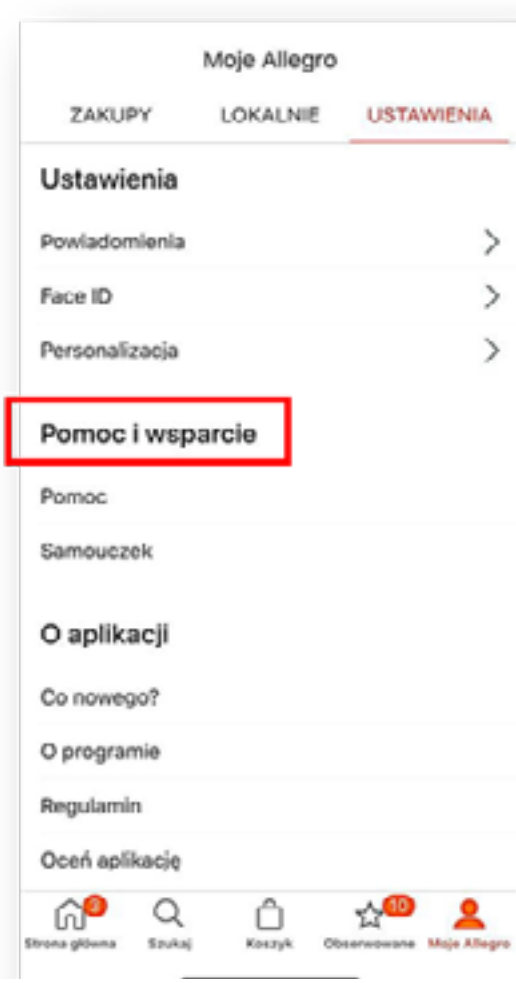
a) wyłączyć usługę Abonamentów dla Sprzedających;
b) uregulować saldo na koncie Allegro, a następnie zamknąć konto;
c) wypłacić środki z Allegro Finanse;
d) uregulować ewentualne zaległości wobec Allegro.

Jeżeli użytkownik wykona wszystkie powyższe kroki to powinien w celu rozwiązania umowy wypełnić stosowny formularz. Serwis po dokonaniu weryfikacji usunie konto.

Uwaga: musimy pamiętać, że Allegro obowiązane jest na podstawie kodeksu cywilnego do przetwarzania danych przez 3 lata (od zakończenia roku, w którym nastąpiło rozwiązanie umowy) - tylko w przypadku jeśli robiłeś zakupy poprzez serwis. W momencie gdy sprzedawałeś lub wykorzystywałeś kupon, okres ten wydłuża się do 6 lat (od zakończenia roku, w którym nastąpiło rozwiązanie umowy).

6.2 Allegro – urządzenia mobilne

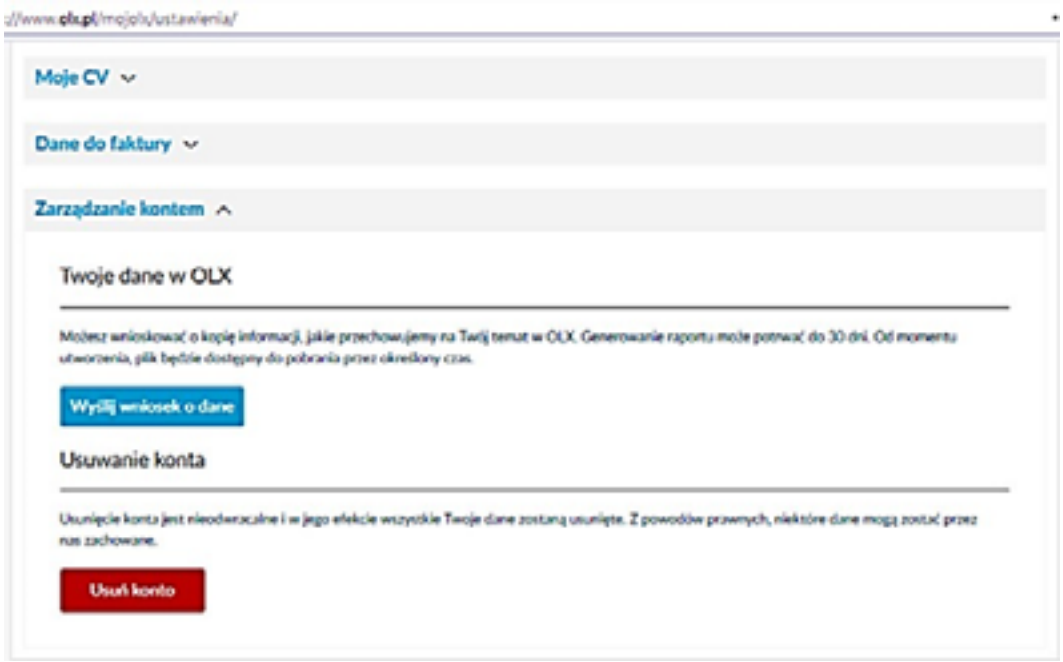
Uwaga: serwis nie umożliwia rezygnacji z usług za pośrednictwem dedykowanej aplikacji na urządzenia mobilne. Możesz jednak znaleźć przydatne informacje w „Ustawieniach” pod przyciskiem „Moje Allegro”, zgodnie z poniższym zrzutem ekranu:



Rysunek 26. Pomoc i wsparcie w aplikacji mobilnej Allegro.

6.3 OLX – urządzenia stacjonarne

Zgodnie z regulaminem OLX, każdy użytkownik może w dowolnym momencie usunąć konto i tym samym rozwiązać umowę z serwisem. Będąc zalogowanym na swoim koncie, w zakładce „Zarządzanie kontem” należy wybrać opcję „Usuń konto”. Następnie należy potwierdzić chęć usunięcia konta poprzez kliknięcie linka z potwierdzeniem przesłanego na e-maila.



Rysunek 27. Panel zarządzanie kontem w OLX.

Jeżeli chcemy, aby serwis zaprzestał przetwarzania danych z konta, należy kliknąć „Zapomnij mnie". Pamiętaj jednak, że po wykonaniu tej czynności, nie będzie możliwe jej cofnięcie.

6.4 OLX – urządzenia mobilne

OLX oferuje również pełne usunięcie konta z poziomu aplikacji mobilnej6. Jest to bardzo proste i sprowadza się do wykonania zaledwie kilku kroków, zgodnie z poniższym schematem:

Rysunek 28. Schemat przedstawiający usunięcie konta w mobilnej aplikacji OLX.

Panel ustawień wygląda w następujący sposób, zgodnie zrzutem ekranu:

Rysunek 29. Opcja usunięcia konta na platformie OLX

7 Usunięcie kont w usługach świadczonych przez Google

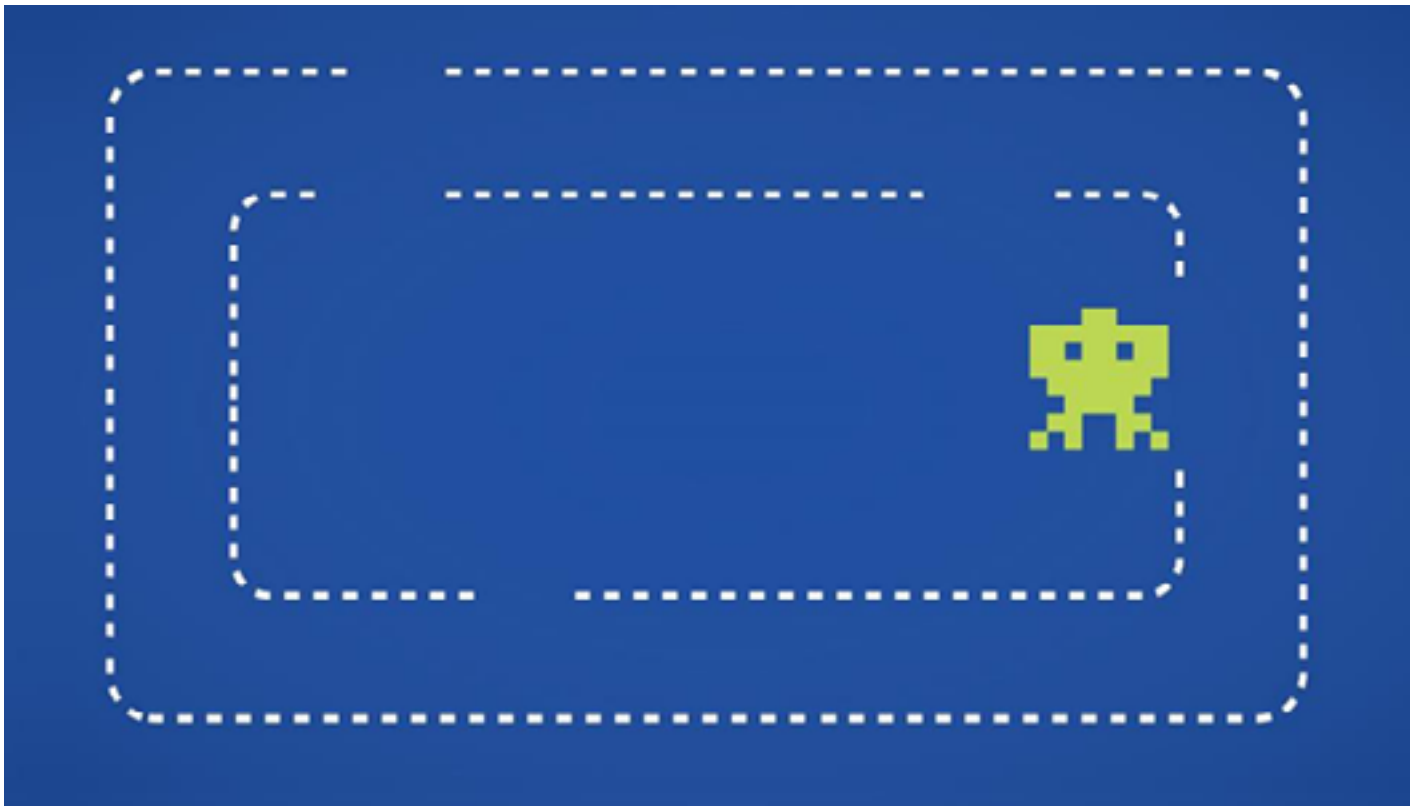
Usunięcie konta Google powoduje wyczyszczenie wszystkich danych powiązanych z tym kontem i używanymi usługami, np. Gmail, Google Play czy YouTube. Jest jednak bardzo proste i w praktyce sprowadza się do kilku kroków. Warto jednak dobrze się zastanowić przed podjęciem takiej decyzji. Usługi Google są na tyle popularne, że nawet chwilowe usunięcie konta może stanowić dla spory problem w poruszaniu się po cyfrowym świecie. Jeśli jednak jest to świadoma decyzja, postępuj zgodnie z instrukcją:

1. w celu trwałego usunięcia konta Google zaloguj się na swoim koncie;
2. wybierz „Aplikacje Google” (prawy górny róg ekranu przeglądarki), a następnie
a. „Konto” – przycisk ten występuje jako ikona twojego awatara;
3. wybierz opcję „Dane i personalizacja”, a następnie w sekcji „Pobierz lub usuń swoje dane albo zaplanuj, co ma się z nimi stać” kliknij „Usuń usługę lub swoje konto”. Masz do dyspozycji różne opcje. Możesz usunąć wybraną usługę Google’a, pobrać swoje dane (utworzyć archiwum) lub zaplanować co ma się stać z nieaktywnym kontem. Oczywiście możliwe jest też **trwałe usunięcie konta**:

Rysunek 29. Usuwanie konta Google.

Jeśli użytkownik chce całkowitego usunięcia konta i wszystkich usług z nim związanych, musi wybrać tę opcję. Google poprosi użytkownika o ponowne wprowadzenie hasła.

Warto zapoznać się uwagami, o których informuje Google w kontekście usuwania konta. Przywrócenie konta może być niemożliwe, stracimy też dostęp do wszystkich usług, z których korzystamy za pomocą loginu Google (np. YouTube, Kalendarz, Google Play).



8 Usuwanie danych użytkownika z różnych for i sklepów internetowych, gier online i platform blogowych

Case study

Pan Krzysiek w młodości był radykalnym aktywistą ekologicznym. Jeszcze w czasach szkoły średniej, jako wolontariusz brał udział w sesjach zdjęciowych przebrany za zwierzęta i rośliny, promując ekologiczny tryb życia. Od czasu tamtych wydarzeń minęło już parę lat, ale w sieci nadal można znaleźć zdjęcia przedstawiające jego wizerunek. Pan Krzysiek ukończył studia na kierunku "Ochrona środowiska" i rozpoczął pracę w branży związanej z przemysłem rolniczym. Obecnie woli nie być kojarzony z radykalnymi organizacjami ekologicznymi.

Rozwiązanie: W zależności od tego, jak była skonstruowana umowa Pana Krzyśka z organizacją ekologiczną, może on wystąpić z żądaniem o wstrzymanie przetwarzania oraz usunięcia danych osobowych.

Każdy z użytkowników internetu korzysta z niego nie tylko w życiu zawodowym, ale również realizując swoje prywatne pasje. Użytkownicy w tym celu bardzo często rejestrują się na różnych forach tematycznych i w witrynach sklepów internetowych lub serwisach z grami online; niekiedy prowadzą bloga na wielu dostępnych platformach blogowych czy portalach społecznościowych. Dostawcy tego typu usług umożliwiają usunięcie konta w sposób mniej lub bardziej zbliżony do przypadków opisanych powyżej.

Zdarzają się jednak i takie, które nie przewidują możliwości usunięcia swojego konta przez samego użytkownika. Jak powinien on wtedy postąpić, by trwale usunąć swoje dane?

Użytkownik powinien skorzystać z prawa do bycia „zapomnianym”, które to prawo omówione zostało w rozdziale 3. tego podręcznika („Informacje Prawne”).

Administrator powinien wykonać czynności wstrzymania przetwarzania danych i ich usunięcia bez zbędnej zwłoki. Również w tym wypadku użytkownik żądający usunięcia danych musi pamiętać, że administrator danych osobowych nie ma takiego obowiązku, o ile żądanie dotyczy danych, których tryb uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy. W innym przypadku, kiedy administrator danych osobowych nie wstrzymał się z przetwarzaniem danych użytkownika i nie usunął ich, osoba, której dane dotyczą, może zwrócić się bezpośrednio do Prezesa Urzędu Ochrony Danych Osobowych (PUODO) ze skargą na administratora na naruszenie przez niego wymogu ochrony danych osobowych.

9 Procedura zgłaszania do organu nadzorczego skargi na naruszenie ochrony danych osobowych

W przypadku naruszenia przepisów dotyczących danych osobowych, można złożyć skargę bezpośrednio do organu nadzorczego, jakim jest Prezes Urzędu Ochrony Danych Osobowych.

Prawo do złożenia skargi reguluje art. 77 Rozporządzenia 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 w brzmieniu:

a) bez uszczerbku dla innych administracyjnych lub środków ochrony prawnej przed sądem każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza niniejsze rozporządzenie;
b) organ nadzorczy, do którego wniesiono skargę, informuje skarżącego o postępach i efektach rozpatrywania skargi, w tym o możliwości skorzystania z sądowego środka ochrony prawnej na mocy art. 78.

Skargę można złożyć zarówno drogą elektroniczną jak i tradycyjną, poprzez wysłanie jej listem, lub dostarczenie osobiście do PUODO. Dodatkowo możliwe jest zgłoszenie skargi

ustnie do protokołu w siedzibie organu nadzorczego w godzinach jego urzędowania.

Droga tradycyjna

Skargę do PUODO składa się w zasadzie tak samo jak do wszystkich innych urzędów, czyli w formie pisemnej. Każda skarga musi zawierać:

- imię i nazwisko oraz adres zamieszkania.
- wskazanie podmiotu, na który skarga zostaje złożona (nazwę/imię i nazwisko oraz adres siedziby/zamieszkania).
- dokładny opis naruszenia.
- żądanie – jakich działań skarżący oczekuje od PUODO (np. usunięcia danych, wypełnienia obowiązku informacyjnego, sprostowania danych, ograniczenia przetwarzania danych itd.).
- własnoręczny podpis.

Osoba składająca skargę powinna pamiętać, by do zgłoszenia dołączyć dowody potwierdzające nieprawidłowe działanie administratora danych osobowych (np. korespondencję z administratorem, umowy, zaświadczenia).

Droga elektroniczna

Skargę możemy złożyć przez Elektroniczną Skrzynkę Podawczą Prezesa Urzędu Ochrony Danych Osobowych.

Skarga składana w formie elektronicznej, oprócz wymogów dla skargi w formie pisemnej, musi zawierać adres elektroniczny skarżącego.

Należy zwrócić uwagę na to, że skarga składana drogą elektroniczną powinna być podpisana kwalifikowanym podpisem elektronicznym albo podpisem elektronicznym potwierdzonym profilem zaufanym ePUAP. Kliknij tutaj, aby uzyskać więcej informacji o profilu zaufanym.

10 Nieskuteczne praktyki

Internautom wydaje się często, że poprzez wykonanie jakiegoś działania usuną na zawsze informacje umieszczone przez siebie w sieci. Faktycznie są to jednak tylko działania pozorne, nie gwarantujące faktycznego usunięcia danych. Poniżej przedstawimy najczęściej spotykane przykłady takich działań:

- użytkownik musi być świadomy, że nie zapewni faktycznego usunięcia swoich prywatnych danych poprzez proste skasowanie swoich zdjęć z popularnych portali społecznościowych, gier online, blogów, forów, stron internetowych i witryn e-sklepów. Bardzo często znikają one tylko z publicznej warstwy strony internetowej, ale jeśli ktoś poświęci na ich odszukanie trochę czasu i pracy, będzie w stanie do nich dotrzeć.
- podobnie jest z komentarzami, czy opiniami zamieszczanymi w sieci. Użytkownik nie zapewni usunięcia swoich prywatnych danych poprzez wykasowanie wszelkich swoich wpisów/komentarzy - zarówno na popularnych portalach społecznościowych, grach online, blogach, jak również forach i stronach internetowych czy witrynach sklepów online. Do wszystkiego, co na pierwszy rzut oka jest niewidoczne, można dotrzeć.
- często użytkownikowi wydaje się, że jeśli wyloguje się z jakiegoś konta i zaprzestanie jego użytkowania, to po jakimś czasie jego dane zostaną usunięte. Nic bardziej mylnego. Nie zapewnimy usunięcia swoich prywatnych danych poprzez wylogowanie się z konta.

- co jakiś czas w sieci pojawiają się tzw. łańcuszki, w których użytkownik oświad-

cza swoją wolę publikując tego typu deklarację na swoim profilu. Nigdy nie zapewnimy usunięcia swoich prywatnych danych poprzez napisanie na swoim profilu oświadczenia o cofnięciu zgody na przetwarzanie danych osobowych. Dotyczy to popularnych portali społecznościowych, gier online, blogów, forów i stron internetowych, czy też sklepów i usług online.

- częstym popełnianym przez użytkowników błędem jest zmiana danych na swoich profilach administratora konta. Należy pamiętać, że na pewno nie zapewnimy usunięcia swoich prywatnych danych poprzez taką zmianę. Nasze poprzednie dane będą nadal dostępne w sieci.
- nie zapewnimy usunięcia naszych prywatnych danych poprzez zerwanie umowy o świadczenie usługi dostępu do internetu.

11 Przydatne linki

- RODO – informacje, gov.pl
- GDPR, gdpr-info.eu
- Po co są ciasteczka?, wszystkoociasteczkach.pl
- Jak strony śledzą użytkowników? Zgodnosczrodo.pl
- Jak trwale usunąć konto?, Facebook.com
- Usunięcie informacji z Google, Google.com
- Kiedy i jak mogę usunąć swoje dane osobowe z Allegro? Allegro.pl
- Jeśli chcesz złożyć skargę, Prezes Urzędu Ochrony Danych Osobowych,
- Zasady Twittera

UKE