

PO CO JEST TO RODO?

RODO weszło w życie pięć lat temu i mimo upływu czasu nadal nie bardzo wiemy po co je wprowadzono

Niniejsza prezentacja stanowi początek cyklu prezentacji mających przybliżyć dobre praktyki ochrony danych w Sektorze Medycznym

Po co właściwie jest to RODO...?

Zapewne niejednokrotnie słyszeliśmy lub zadawaliśmy sobie pytanie ***Po co jest RODO?***

Przez ostatnie 20 lat obserwowaliśmy gwałtowny rozwój technologii informatycznej. Serwisy społecznościowe, sprzedaż internetowa, usługi mobilne, chmury obliczeniowe - to jedne z tych usług internetowych, które powodują, że nasze dane osobowe są przetwarzane i wykorzystywane na coraz więcej sposobów. Tym samym nasza prywatność jest coraz słabiej chroniona, a my często tracimy kontrolę nad informacjami na swój temat. Badania prowadzone przez Komisję Europejską ujawniły, że **ponad 75% Europejczyków nie ufała portalom społecznościowym i wyszukiwarkom internetowym, 50% obawiała się, że stanie się ofiarą oszustwa polegającego na niewłaściwym wykorzystaniu danych na ich temat, a zaledwie 15% przyznało, że ma poczucie pełnej kontroli nad swoimi danymi.** Między innymi te liczby przemawiały za koniecznością znowelizowania obowiązującego od 1995 roku unijnego prawa w zakresie danych osobowych.

O potrzebie RODO niech świadczy największy skandal dotyczący operacji na danych...



Po co jest RODO?

Cambridge Analytica Ltd była brytyjską firmą doradztwa politycznego, która zyskała rozgłos dzięki skandalowi związanemu z danymi Facebooka. Firma zamknęła działalność w 2018 roku, gdy dane osobowe użytkowników Facebooka zostały pozyskane za pośrednictwem aplikacji o nazwie „THIS IS YOUR DIGITAL LIFE”. W 2015 r. dało to tej aplikacji dostęp również do informacji o znajomych użytkownika i skutkowało zgromadzeniem danych około 87 milionów użytkowników, z których większość nie udzieliła jednoznacznie zgody Cambridge Analytica na dostęp do swoich danych.

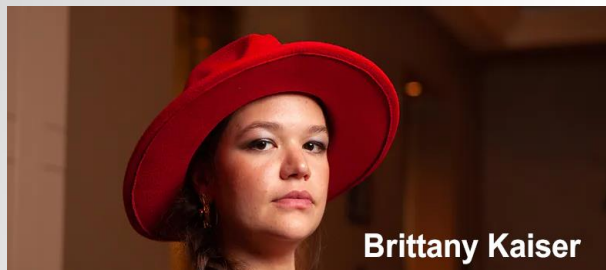
Poniższe treści zostały „wyjęte” z artykułu Krzysztofa Majdana opublikowanego 15.11.2021 na stronie money.pl

<https://www.money.pl/gospodarka/byla-zwiazana-z-najwieksza-afra-ostatnich-lat-zdradzila-nam-jak-pralo-sie-ludziom-mozgi-na-ogromna-skale-6703329326820224a.html>

„Cambridge Analytica to firma specjalizująca się w propagandzie prowadzonej z cienia na ogromną skalę. To oni zapewnili Trumpowi fotel prezydencki, to oni tak zakręcili Brytyjczykami, że sami wyprowadzili się z Unii Europejskiej. (...)”

Afera pokazała, z jaką łatwością można prać ludziom mózgi na ogromną skalę, zmieniając ich wydawałoby się twarde poglądy, i pozostać do tego niezauważonym. Choć od wybuchu afery minęło parę lat, długo się jeszcze będzie ciągnąć. Pod koniec października tego roku (2021) Mark Zuckerberg trafił na listę oskarżonych w tej sprawie.(...)

(...) **Brittany Kaiser** jest jedną z bohaterek głośnego filmu dokumentalnego Netfliksa - "The Great Hack", napisała też książkę o bezpieczeństwie danych, wydaną w Polsce przez Krytykę Polityczną. Przy okazji konferencji Infoshare, dziennikarz money.pl miał okazję z nią porozmawiać.(...)



Brittany Kaiser

Rozmowa z Brittany

Łatwo uderzyć w czyjś emocjonalny puls? Jak spróbowałabyś zmienić moje zachowanie albo przekonanie?

Nie powiedziałabym, że łatwo. Chyba że masz dostęp do tak wielu danych tej osoby, jak to możliwe. Co czytałeś w ostatnich miesiącach, na jakich zdjęciach zatrzymujesz wzrok na dłużej, gdy przewijasz palcem po telefonie. Wtedy wiem, gdzie jest twój słaby punkt, co cię angażuje lub porusza. I na tej podstawie konstruuje przekaz, wycelowany bezpośrednio w ciebie.

A jeśli nie zadziała? Na przykład z powodu oślego uporu?

Wtedy mogę opracować algorytm, który stworzy różne warianty tego spreparowanego pod ciebie przekazu. Będzie ci je tak długo pokazywał w różnych konfiguracjach, aż cię w końcu zaangażuje. Później robi to znowu. I znowu. A mówimy tylko o tobie. Technologia pozwala robić to na dużą skalę, całe grupy zamiast pojedynczych osób. Wiele firm technologicznych zatrudnia psychologów, żeby nauczyć algorytmy, co rusza ludzi. Testują, testują, testują, aż w końcu trafią w odpowiednią emocję.

Czy kiedykolwiek prowadziliście jakieś działania w Polsce lub dla polskich podmiotów?

Dostawaliśmy zapytania, głównie od firm, ale też z dwóch partii politycznych. Nie podjęliśmy się żadnego zlecenia, przynajmniej dopóki ja tam pracowałam, bo przepisy bardzo by je utrudniały.

Najbliższe wybory parlamentarne w Polsce zaplanowano na 2023 r. Ile firma jak CA potrzebowałaby, żeby w nich namieszać?

Prezes Cambridge Analytica Alexander Nix zwykł mawiać, że w 6 miesięcy możesz wyrzucić silny wpływ. W 9 miesięcy wywołasz dający się przewidzieć efekt. A jeśli masz 2 lata, to w zasadzie gwarantujesz zwycięstwo w wyborach.”(...)

Zachęcam do obejrzenia filmu i przeczytania artykułu



Kradzież tożsamości

Źródło:

<https://bialystok.naszemiasto.pl/michal-cira-ciruk-zgubil-dokumenty-teraz-ma-problem-z/ar/c1-4647955>

Michał "Cira" Ciruk zgubił dokumenty i teraz ma duże problemy. Białostocki raper dwa lata temu zgubił swój portfel. Dowód osobisty szybko zablokował. Niestety zrobił to tylko w urzędzie, a powinien jeszcze zgłosić to w banku. Kilka tygodni po tym zdarzeniu zaczął otrzymywać pisma od firm kredytowych oraz banków. Pisaliśmy już o tym dwa lata temu: **Michał "Cira" Ciruk tłumaczy się za długi. Cudze!**

Wezwania do zapłaty, ponaglenia, maile, telefony, pukanie do drzwi. Oczywiście domyśliłem się, że ktoś w najlepsze bierze pożyczki na mój ZABLOKOWANY dowód - napisał na swoim profilu Michał Ciruk.

Białostocki raper bardzo mocno przeżywa całą sytuację. Ma kłopoty ze snem i z żołądkiem. Był u psychiatry, bo wciąż prześladują go natrętne myśli i "pokutowanie za coś, czego nigdy nie zrobiłem". Michał Ciruk dostawał lub wciąż dostaje pisma i ponaglenia od 25 firm.

Trwają postępowania sądowe wobec mojej osoby. W jednych jestem oskarżonym, w innych poszkodowanym. Dzień w dzień dzwonią do mnie z banków i parabanków. Przestałem odbierać obce numery. Boję się zaglądać do skrzynki na listy. Nienawidzę podwójnego dźwięku domofonu, bo wiem, że to listonosz niesie mi kolejną kopertę pełną bezradności, irytacji i strachu. Dopiero po jakimś czasie Michał Cira zorientował się, że zgubiony dowód osobisty należy zablokować również w swoim banku.

- Żeby nie mój kolega - prawnik, który nieodpłatnie udziela mi pomocy, pewnie siedziałbym już w więzieniu - podsumowuje.

Kradzież tożsamości



Okazuje się jednak, że nie trzeba zgubić dowodu, aby przeżyć to co raper z Białegostoku. Wystarczy, że lekarz wyśle do kolegi lekarza dane pacjenta w tekście e-maila, dołączy ksero skierowania, wynik badania lub inny niezaszyfrowany dokument.

Wystarczy, że dostęp do skrzynki uzyska haker i przejmie ją zupełnie tak samo jak przejęto skrzynkę Michała Dworczyka.

W przeciwieństwie do „Prywatnej rozmowy” nie będzie publikował danych, ale je wykorzysta. Jeśli znajdzie tam imię i nazwisko, PESEL to resztę danych spreparuje i dokona kradzieży tożsamości.

Mimo wprowadzenia obostrzeń kupienie kolekcjonerskiego dowodu tożsamości nie jest niemożliwe



Kradzież tożsamości

USTAWA z dnia 22 listopada 2018 r. o dokumentach publicznych wprowadziła przepis:
Art. 58. Kto wytwarza, oferuje, zbywa lub przechowuje w celu zbycia replikę dokumentu publicznego, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Przepis ten miał zapobiec obrotowi podrobionych dowodów osobistych, ale istnieją nadal strony internetowe, które oferują takie dowody za ok 800 zł.

Widać tutaj prostą drogę **od lekarza** - który zlekceważył Zasady Ochrony Danych **przez przestępcę** - który to wykorzystał; **do poszkodowanego pacjenta**.

Pacjent, gdy się zorientuje, że z winy szpitala przechodzi to, co białostocki raper, zażąda odszkodowania za poniesione szkody na podstawie art. 82 RODO.



Parlament Europejski

Art. 82 - Prawo do odszkodowania i odpowiedzialność

1. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.
2. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.
3. Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.
4. Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i zgodnie z ust. 2 i 3 odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.
5. Administrator lub podmiot przetwarzający, który zgodnie z ust. 4 zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w ust. 2.
6. Postępowanie sądowe dotyczące odszkodowania jest wszczynane przed sądem właściwym na mocy prawa państwa członkowskiego, o którym mowa w art. 79 ust. 2.

Proszę odpowiedzieć na pytanie



Jaka szafa lepiej chroni dane? Żelazna czy drewniana?

Obojętnie z czego będzie zrobiona, gdy jej nie zamkniemy!

Do ochrony danych możemy użyć różnych środków. Od bardzo prostych do bardzo wyrafinowanych. Możemy stworzyć niezwykle skomplikowany i drogi system zabezpieczeń, a i tak o jego skuteczności zdecyduje beztroska, lenistwo, ignorancja lub brak wyobraźni kogoś z personelu.

Sukces zależy od tego, czy uda nam się **dotrzeć do świadomości** lekarzy, pielęgniarek, położnych, fizjoterapeutów, ratowników medycznych, laborantów oraz innych osób przetwarzających dane i przekonać je, że ochrona danych ma sens i leży w ich interesie.

Udowadnia to następny slajd ...



Słabe ogniwa

Kevin David Mitnick - już jako nastolatek swoimi umiejętnościami zastraszył całą Amerykę. Z czasem stał się **najstydniejszym hakerem świata** i wrogiem publicznym numer jeden

- okrzyknięty przez media groźnym cyberprzestępcą, gorliwie ścigany przez FBI, w końcu podstępem namierzony, osaczony i spektakularnie ujęty...

Uzbrojony w klawiaturę został uznany **za groźnego dla społeczeństwa** - wyrokiem sądu na wiele lat pozbawiono go dostępu do komputera, Internetu i telefonów komórkowych. Jakim sposobem udało mu się włamać do systemów takich firm, jak Nokia, Novell czy Sun Microsystems?!

Ludzka naiwność, łatwowierność i ignorancja - oto najslabsze ogniwa, wiodące do uzyskania poufnych informacji, tajnych kodów i haseł.

Mitnick, w książce „**Sztuka podstępu – łamałem ludzi nie hasła**” przestrzega i pokazuje, jak łatwo można ominąć bariery systemów wartych miliony dolarów. Przedstawiając i analizując metody hakerów oparte na prawdziwych atakach, demonstruje, że tam, gdzie nie można znaleźć luk technicznych, zawsze skuteczne okazują się ludzkie słabości...



Parlament Europejski

PO CO RODO?

Parlament Europejski i Rada Unii Europejskiej pracowały nad zmianami przez cztery lata, dając państwom Unii Europejskiej kolejne dwa lata na jej wprowadzenie w swoich krajach. Finalnie Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO) w Polsce zaczęło obowiązywać od 25 maja 2018 roku.

Celem twórców RODO było:

- doprowadzenie do pełnej harmonizacji prawa w ramach UE i swobodnego przepływu danych osobowych. RODO w założeniu ma pozwolić mieszkańcom Unii Europejskiej **na lepszą kontrolę ich danych osobowych** oraz stanowić modernizację i ujednolicenie przepisów umożliwiających firmom ograniczanie biurokracji i korzystanie ze zwiększonego zaufania klientów.
- Ma też na celu zaktualizować przepisy, by te spełniały swoją funkcję w XXI wieku i odpowiadały na **zagrożenia wynikające z użycia w przetwarzaniu danych osobowych nowoczesnych technologii**.

RODO zostało przyjęte 27 kwietnia 2016. W momencie wejścia w życie, po dwuletnim okresie przejściowym, zaczęło obowiązywać w krajach członkowskich UE bezpośrednio, bez potrzeby wydawania aktów prawnych wdrażających je do porządku krajowego. Zastąpiło wówczas dyrektywę 95/46/WE.

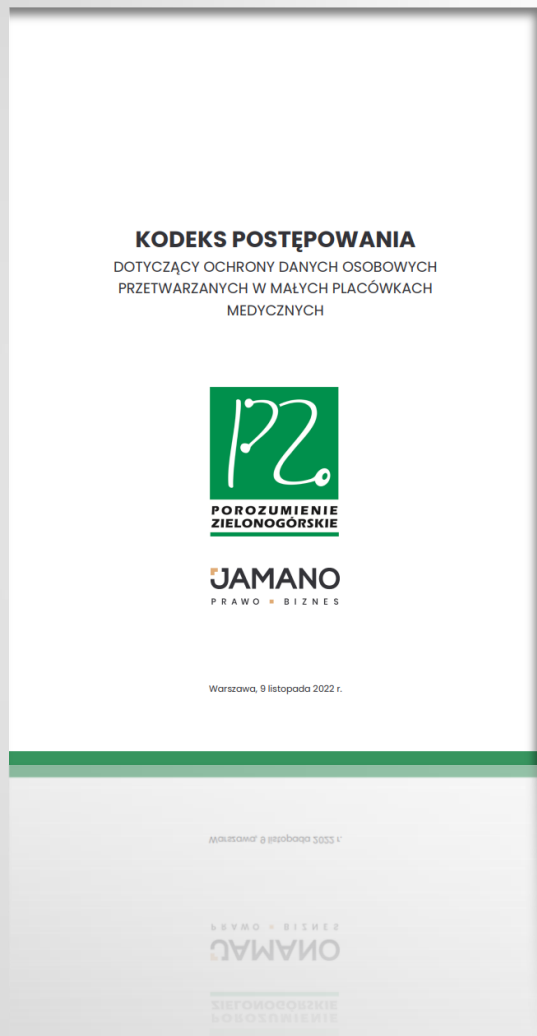
RODO nie mówi jak!

RODO nie mówi nam jak mamy chronić dane. Każe użyć adekwatnych środków.

Nie zostawia nas jednak bez pomocy, gdyż w art. 40 stanowi: Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do sporządzania **kodeksów postępowania** mających pomóc we właściwym stosowaniu niniejszego rozporządzenia – z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Taki **KODEKS POSTĘPOWANIA DOTYCZĄCY OCHRONY DANYCH OSOBOWYCH PRZETWARZANYCH W MAŁYCH PLACÓWKACH MEDYCZNYCH** już powstał i 14.12.2022 r. został zatwierdzony przez Prezesa UODO.

W następnych prezentacjach będę cyklicznie zapoznawał Państwa z jego zapisami, abyśmy wiedzieli jak chronić dane i nie wykazywali się słabościami wyśmiewanymi przez Mitnicka.



Dziękuję za uwagę