RODO


RODO
25.05.2018
ROZPORZĄDZENIE O OCHRONIE
DANYCH OSOBOWYCH


Rodos
Faliraki
Φαληράκι
Κολύμπια
Lindos
Λίνδος


PBR

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)

Zgodnie z art. 99 ogólnego rozporządzenia o ochronie danych, rozporządzenie będzie stosowane od dnia 25 maja 2018 r.

I

(Akty ustawodawcze)

ROZPORZĄDZENIA

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)

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ([1]),

uwzględniając opinię Komitetu Regionów ([2]),

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([3]),

a także mając na uwadze, co następuje:

(1) Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „Kartą praw podstawowych") oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

(2) Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych nie mogą – niezależnie od obywatelstwa czy miejsca zamieszkania takich osób – naruszać ich podstawowych praw i wolności, w szczególności prawa do ochrony danych osobowych. Niniejsze rozporządzenie ma na celu przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, do postępu społeczno-gospodarczego, do wzmacniania i konwergencji gospodarek na rynku wewnętrznym, a także

a także mając na uwadze, co następuje:
(1) Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „Kartą praw podstawowych") oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.
(2) Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych nie mogą – niezależnie od obywatelstwa czy miejsca zamieszkania takich osób – naruszać ich podstawowych praw i wolności, w szczególności prawa do ochrony danych osobowych. Niniejsze rozporządzenie ma na celu przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, do postępu społeczno-gospodarczego, do wzmacniania i konwergencji gospodarek na rynku wewnętrznym, a także do pomyślności ludzi.
(3) Celem dyrektywy Parlamentu Europejskiego i Rady 95/46/WE (4) jest zharmonizowanie ochrony podstawowych praw i wolności osób fizycznych w związku z czynnościami przetwarzania oraz zapewnienie swobodnego przepływu danych osobowych między państwami członkowskimi.

(173) Niniejsze rozporządzenie powinno mieć zastosowanie do wszystkich tych kwestii dotyczących ochrony podstawowych praw i wolności w związku z przetwarzaniem danych osobowych, które nie podlegają szczególnym obowiązkom mającym ten sam cel określonym w dyrektywie Parlamentu Europejskiego i Rady 2002/58/WE (2), w tym obowiązkom nałożonym na administratora oraz prawom osób fizycznych. Aby doprecyzować związek między niniejszym rozporządzeniem a dyrektywą 2002/58/WE, dyrektywę tę należy odpowiednio zmienić. Gdy niniejsze rozporządzenie zostanie przyjęte, dyrektywa 2002/58/WE powinna zostać poddana przeglądowi, w szczególności w celu zapewnienia jej spójności z niniejszym rozporządzeniem,

(173) Niniejsze rozporządzenie powinno mieć zastosowanie do wszystkich tych kwestii dotyczących ochrony podstawowych praw i wolności w związku z przetwarzaniem danych osobowych, które nie podlegają szczególnym obowiązkom mającym ten sam cel określonym w dyrektywie Parlamentu Europejskiego i Rady 2002/58/WE [2], w tym obowiązkom nałożonym na administratora oraz prawom osób fizycznych. Aby doprecyzować związek między niniejszym rozporządzeniem a dyrektywą 2002/58/WE, dyrektywę tę należy odpowiednio zmienić. Gdy niniejsze rozporządzenie zostanie przyjęte, dyrektywa 2002/58/WE powinna zostać poddana przeglądowi, w szczególności w celu zapewnienia jej spójności z niniejszym rozporządzeniem,

---

([1]) Dz.U. C 192 z 30.6.2012, s. 7.
([2]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

Przepisy ogólne

Artykuł 1

Przedmiot i cele

1. W niniejszym rozporządzeniu ustanowione zostają przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych.

2. Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych.

3. Nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

Artykuł 2

Materialny zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

2. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:

Artykuł 4
Definicje

Na użytek niniejszego rozporządzenia:

1) „dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

2) „przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie,
ograniczanie, usuwanie lub niszczenie;

3) „ograniczenie przetwarzania” oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

4) „profilowanie” oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
5) „pseudonimizacja” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe
informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
6) „zbiór danych” oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

7) „administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
8) „podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
9) „odbiorca” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
10) „strona trzecia” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

11) „zgoda” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
12) „naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
13) „dane genetyczne” oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
14) „dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
15) „dane dotyczące zdrowia” oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;

Artykuł 7

Warunki wyrażenia zgody

1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

2. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.

3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

Artykuł 9

Przetwarzanie szczególnych kategorii danych osobowych

1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Artykuł 99

Wejście w życie i stosowanie

1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po publikacji w Dzienniku Urzędowym Unii Europejskiej.

2. Niniejsze rozporządzenie ma zastosowanie od dnia 25 maja 2018 r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 27 kwietnia 2016 r.

Opracowano na podstawie: t.j. Dz. U. z 2019 r. poz. 1781.

U S T A W A

z dnia 10 maja 2018 r.

o ochronie danych osobowych[1), 2)]

Rozdział 1

Przepisy ogólne

Art. 1. 1. Ustawę stosuje się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w zakresie określonym w art. 2 i art. 3 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679".

2. Ustawa określa:

1) podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o jego wyznaczeniu;
2) warunki i tryb akredytacji podmiotu uprawnionego do certyfikacji w zakresie ochrony danych osobowych, akredytowanego przez Polskie Centrum Akredytacji, zwanego dalej „podmiotem certyfikującym", podmiotu monitorującego kodeks postępowania oraz certyfikacji;
3) tryb zatwierdzenia kodeksu postępowania;

---

1) Niniejsza ustawa służy stosowaniu 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 (ogólne rozporządzenie o ochronie danych).

2) Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania

Dz.U. 1997 nr 133 poz. 883

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Tekst ogłoszony:	D19970883.pdf
Tekst ujednolicony:	D19970883Lj.pdf
Status aktu prawnego:	uchylony
Data ogłoszenia:	1997-10-29
Data wydania:	1997-08-29
Data wejścia w życie:	1998-04-30
Data obowiązywania:	1998-04-30
Data uchylenia:	2018-05-25
Organ wydający:	SEJM
Organ zobowiązany:	MIN. SPRAW WEWNĘTRZNYCH I ADMINISTRACJI

Urząd Ochrony Danych Osobowych

Aktualności

ormacje dostępne w zakładce: Prezes i Urząd/Praca.

15.02.2019 r.

Przy sprzedaży węgla dochodzi do nadmiarowego pozyskiwania danych nabywców

Prezes UODO wystąpiła do Ministra Finansów z prośbą o zmianę przepisów, które wymuszają na sprzedawcach węgla zbieranie od nabywców zbyt szerokiego zakresu ich danych osobowych.

15.02.2019 r.

W oku kamery. Monitoring wizyjny – Prezes UODO wyjaśnia, jak go obecnie stosować

– Monitoring jest jedną z najbardziej inwazyjnych form przetwarzania danych osobowych i powinien być stosowany jedynie w sytuacji, gdy nie istnieją inne, mniej ingerujące w prywatność środki umożliwiające zapewnienie bezpieczeństwa – tłumaczy w filmie edukacyjnym pt. „W oku kamery. Monitoring wizyjny" dr Edyta Bielak, Prezes Urzędu Ochrony Danych Osobowych.

14.02.2019 r.

Ochrona danych osobowych w kościołach i związkach wyznaniowych

Kościoły i związki wyznaniowe nie mają pełnej autonomii przy tworzeniu swoich regulacji o ochronie danych – muszą być one dostosowane do RODO. Dlatego Prezes UODO wspiera je przy tworzeniu tych regulacji. Te związki wyznaniowe, które nie zdecydowały się na wprowadzenie odrębnych regulacji o ochronie danych, muszą pamiętać, że całkowicie podlegają pod RODO - powiedziała Prezes Urzędu Ochrony Danych Osobowych, dr Edyta Bielak-Jomaa podczas briefingu prasowego poświęconemu problematyce danych osobowych w kościołach i związkach wyznaniowych w świetle RODO.

13.02.2019 r.

Ruszyła Infolinia UODO dla IOD

Urząd Ochrony Danych Osobowych uruchomił specjalną infolinię dedykowaną inspektorom ochrony danych (IOD). Im wyższa jest fachowa wiedza i doświadczenie inspektora ochrony danych, tym większa szansa na zbudowanie w organizacji, która go wyznaczyła, skutecznego systemu ochrony danych osobowych.

Prezes Urzędu Ochrony Danych Osobowych

Prezesem Urzędu Ochrony Danych Osobowych jest doktor nauk prawnych Edyta Bielak–Jomaa.

Bezpośrednio przed objęciem tej funkcji Edyta Bielak–Jomaa pełniła obowiązki Generalnego Inspektora Ochrony Danych Osobowych. Sejm powołał ją na to stanowisko 9 kwietnia 2015 r., a Senat zaakceptował ten wybór 16 kwietnia 2015 r.

Edyta Bielak – Jomaa urodziła się 10 maja 1972 r. w Sandomierzu. Jest absolwentką Wydziału Prawa i Administracji Uniwersytetu Łódzkiego (WPiA UŁ). W 2003 r. uzyskała stopień doktora nauk prawnych i została zatrudniona w Katedrze Prawa Pracy WPiA UŁ na stanowisku adiunkta. Od 2012 r. do kwietnia 2015 r., czyli do czasu powołania na stanowisko Generalnego Inspektora Ochrony Danych Osobowych, pełniła funkcję Kierownika Podyplomowych Studiów Ochrony Danych Osobowych WPiA UŁ, a od 2013 r. Kierownika Centrum Ochrony Danych Osobowych i Zarządzania Informacją.

Była wykładowcą z zakresu ochrony danych osobowych, prawa pracy i zagranicznych migracji zarobkowych. Pełniła funkcję opiekuna naukowego Międzywydziałowego Koła Studenckiego Praw Osób Niepełnosprawnych, prowadziła szkolenia w ramach działalności Międzynarodowej Fundacji Kobiet oraz cykl szkoleń organizowanych dla pracowników i pracodawców regionu „Różni ale równi" dotyczących równego traktowania oraz zakazu dyskryminacji na rynku pracy.

Była organizatorką konferencji i debat poświęconych problematyce danych osobowych, takich m.in., jak: „Dane medyczne - granice wykorzystywania i ochrona", „Ochrona danych osobowych w działalności Kościołów i innych związków wyznaniowych", „Ochrona danych osobowych a działalność dziennikarska - granice przywileju medialnego", „Ochrona danych osobowych a wykonywanie zawodów prawniczych", „Ochrona danych osobowych a wybory", „Sędzia – osoba publiczna czy prywatna? Granice dostępu do informacji publicznej i ochrony danych osobowych"(współorganizator Prezes Sądu Apelacyjnego w Łodzi oraz Oddział Łódzki Stowarzyszenia Sędziów Polskich IUSTITIA).

Dr Edyta Bielak – Jomaa jest autorką ponad 30 opracowań z zakresu prawa pracy, problematyki rynku pracy, oraz ochrony danych osobowych.

Zainteresowania naukowe obejmują przede wszystkim problematykę ochrony dóbr osobistych pracowników i ochronę danych osobowych w zatrudnieniu. Jako pierwsza rozpoczęła badania nad ochroną danych osobowych bezrobotnych i poszukujących pracy.

2018-05-13

Prezes Urzędu Ochrony Danych Osobowych dr Edyta Bielak–Jomaa

Urząd Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa
fax. 22 531 03 01
Godziny pracy urzędu: 8.00 – 16.00
Infolinia: 606-950-000
czynna w dni robocze od: 10.00 – 13.00

Prezes Urzędu Ochrony Danych Osobowych

Prezesem Urzędu Ochrony Danych Osobowych jest Jan Nowak.

Sejm powołał go na to stanowisko 4 kwietnia 2019 r., a Senat zaakceptował ten wybór 12 kwietnia 2019 r. Od dnia złożenia ślubowania przed Sejmem, tj. od 16 maja 2019 r., zgodnie z ustawą o ochronie danych osobowych, rozpoczęła się czteroletnia kadencja na tym stanowisku.

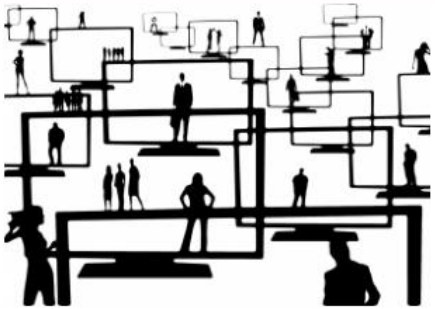
Z ochroną danych osobowych i urzędem jest związany od 2008 roku. Najpierw jako Dyrektor Biura Generalnego Inspektora Ochrony Danych Osobowych, a następnie – do chwili wyboru na stanowisko Prezesa - jako Dyrektor Urzędu Ochrony Danych Osobowych.

Jan Nowak jest absolwentem Politechniki Warszawskiej oraz podyplomowych studiów EMBA w Wyższej Szkole Menadżerskiej w Warszawie.

Aktualności

20.02.2020 r. 18. posiedzenie plenarne Europejskiej Rady Ochrony Danych, 18-19.02.2020 r.

[...]



19.02.2020 r. Stop handlowi bazami danych! Prezes UODO reaguje

Do UODO napływają sygnały o niezgodnych z prawem praktykach pracowników banków, polegających na nielegalnym sprzedawaniu baz danych klientów tych instytucji. [...]

17.02.2020 r. 1% dla OPP

Przed nami okres rozliczeniowy podatku dochodowego za rok 2019. Wielu podatników przekaże kwotę 1% należnego podatku na organizację pożytku publicznego [...]

14.02.2020 r. Nie trać głowy i serca w sieci

Ile razy dzielimy się nadmiernymi danymi na swój temat? Czy zastanawiamy się komu i w jakim celu je udostępniamy? Z [...]

11.02.2020 r. Dane dzieci bezpieczne w sieci

Wraz z rozwojem nowych technologii liczba zagrożeń związanych z utratą danych stale rośnie. Najbardziej narażone na nie są dzieci. Dostęp [...]

10.02.2020 r. Trwają konsultacje wytycznych w sprawie pojazdów połączonych i aplikacji związanych z mobilnością

Do 20 marca 2020 r. Europejska Rada Ochrony Danych (EROD) przyjmuje uwagi do wytycznych 1/2020 poświęconych pojazdom połączonym i aplikacjom [...]

10.02.2020 r. Czy osoba wystawiająca e-receptę może przez telefon podać pacjentowi 4-cyfrowy kod dostępu?

Do Urzędu Ochrony Danych Osobowych zgłaszane są przez placówki medyczne pytania, związane z sytuacjami w których pacjenci proszą telefonicznie o [...]

06.02.2020 r. Jeśli pracodawca prowadzi ZFŚS, dotyczy go także RODO

Żeby przyznać pracownikowi świadczenie z zakładowego funduszu świadczeń socjalnych, pracodawca musi poznać i ocenić sytuację życiową i materialną pracownika oraz [...]


Zgłoszenie naruszenia ochrony danych osobowych
Zgłoś skargę do Urzędu Ochrony Danych Osobowych
Zgłoszenie Inspektora Ochrony Danych Osobowychh (IOD)
Kontakt z Inspektorem Ochrony Danych UODO
Podania, wnioski, petycje – pismo ogólne
Podania, wnioski, petycje - pismo ogólne od osób fizycznych
Kontakt z Zespołem Prasowym (dla mediów)
Wniosek o udostępnienie informacji publicznej

28 stycznia - Dzień Ochrony Danych Osobowych

Dzień Ochrony Danych Osobowych został ustanowiony na dzień 28 stycznia przez Komitet Ministrów Rady Europy. Obchodzony jest w rocznicę sporządzenia Konwencji 108 Rady Europy z dnia 28 stycznia 1981 r. w sprawie ochrony osób w zakresie zautomatyzowanego przetwarzania danych osobowych. Konwencja ta, jest najstarszym aktem prawnym o zasięgu międzynarodowym, który reguluje zagadnienia związane z ochroną danych osobowych.

Ministerstwo Cyfryzacji

RODO

DLA ADMINISTRACJI

„Dane osobowe” oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”).
Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dane osobowe dzielą się na trzy kategorie:
a) dane tzw. zwykłe, takie jak imię, nazwisko, adres zamieszkania, data i miejsce urodzenia, numer telefonu, wykonywany zawód, wizerunek, adres e-mail itp.,
b) szczególne kategorie danych osobowych (uprzednio zwane danymi wrażliwymi), wymienione w art. 9 RODO ujawniające:
- pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych,
- dane genetyczne,
- dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej,
- dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby,
c) dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa wymienione w art. 10 rozporządzenia (uprzednio również zaliczane do danych wrażliwych).

Przetwarzanie danych wrażliwych wiąże się z koniecznością wypełnienia dodatkowych gwarancji ich ochrony ujętych w art. 9 ust. 2 i art. 10 RODO.
RODO zabrania przetwarzania danych wrażliwych, o ile nie jest spełniona jedna z przesłanek wymienionych w art. 9 ust. 2 RODO. Przetwarzanie danych o wyrokach skazujących i czynach zabronionych jest natomiast możliwe jedynie po spełnieniu warunków wskazywanych w art. 10 RODO.

RODO wprowadza obowiązek przestrzegania następujących zasad ochrony danych osobowych, zgodnie z którymi dane osobowe muszą być:
a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zgodność z prawem, rzetelność i przejrzystość);
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (ograniczenie celu);
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych);
d) prawidłowe i w razie potrzeby uaktualniane, a dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, muszą być niezwłocznie usunięte lub sprostowane (prawidłowość);
e) przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (ograniczenie przechowywania);
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (integralność i poufność).

Przetwarzanie danych osobowych zwykłych jest zgodne z prawem wyłącznie wtedy, gdy:
- osoba, której dane dotyczą, wyraziła zgodę na ich przetwarzanie,
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub jest konieczne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej,
- przetwarzanie jest niezbędne do wykonywania zadania realizowanego w interesie publicznym,
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub prawa i wolności osoby, której dane dotyczą. Na przesłankę prawnie uzasadnionego interesu realizowanego przez administratora lub osobę trzecią nie mogą się powołać organy publiczne w ramach wykonywania swoich zadań.

Na szczególną uwagę zasługuje problematyka przetwarzania szczególnych kategorii danych. Przetwarzanie ich jest co do zasady zabronione, aczkolwiek art. 9 ust. 2 RODO przewiduje zamknięty katalog przesłanek, a spełnienie choć jednej uprawnia szkołę do przetwarzania tego rodzaju danych osobowych. W przypadku szkoły będą to najczęściej:

- udzielenie przez osobę, której dane dotyczą, lub przez jej opiekuna prawnego (w przypadku niepełno letnich), wyraźnej zgody na przetwarzanie danych w konkretnym celu lub celach,
- niezbędność przetwarzania danych do wypełnienia obowiązków i wykonywania poszczególnych praw przez administratora lub osobę, której dane dotyczą w dziedzinie prawa pracy, zabezpieczenia socjalnego i społecznego;
- niezbędność przetwarzania danych do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, o ile osoba, której dane dotyczą jest niezdolna do wyrażenia zgody;
- przetwarzanie danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- niezbędność przetwarzania danych ze względów związanych z ważnym interesem publicznym, o ile przepisy nie naruszają istoty prawa do ochrony danych;
- niezbędność przetwarzania danych do celów oceny zdolności pracownika do pracy;
- niezbędność przetwarzania danych do celów archiwalnych w interesie publicznym, do celów badań naukowych, historycznych lub statystycznych.

Jednym z obowiązków wynikającym z RODO jest właściwe zabezpieczenie danych osobowych. Zgodnie z art. 32 RODO, przy uwzględnieniu różnych czynników o charakterze technicznym oraz organizacyjnym, zapewnić należyte bezpieczeństwo przetwarzanych danych oraz prowadzić rejestr czynności przetwarzania.
Przykładowe środki służące zabezpieczeniu danych to:
- pseudonimizacja i szyfrowanie danych osobowych,
- zdolność do zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie uszkodzenia fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

RODO wyróżnia dwie sytuacje, w których może mieć miejsce zbieranie danych osobowych:
-zbieranie danych od osoby, której dane dotyczą (tzw. pierwotne gromadzenie danych osobowych, o którym mowa w art. 13 RODO),
-zbieranie danych nie od osoby, której dane dotyczą (tzw. wtórne gromadzenie danych osobowych, o którym mowa w art. 14 RODO).
W przypadku pierwotnego pozyskiwania danych, ustawodawca przewidział zwolnienie z obowiązku informacyjnego wyłącznie w zakresie, w jakim osoba, której dane dotyczą, dysponuje już informacjami.
W przypadku wtórnego pozyskiwania danych, RODO wymienia cztery przypadki, w których administrator jest zwolniony z obowiązku informacyjnego. Są to sytuacje, gdy:
-osoba, której dane dotyczą, dysponuje już tymi informacjami,
- udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, lub o ile spełnienie tego obowiązku, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W ta-kich przypadkach administrator musi podjąć odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie,
-pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator,
- dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.


Urząd
Ochrony
Danych
Osobowych

Prezes Urzędu przygotował propozycję wykazu rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych. W ostatecznej wersji dokumentu wskazano, jakie operacje przetwarzania przy użyciu monitoringu wizyjnego wymagają przeprowadzenia oceny skutków. Są to:

1) Systematyczne monitorowanie na dużą skale miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajda się w monitorowanej przestrzeni. Do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa

   Środki komunikacji miejskiej, miasta oferujące systemy wypożyczania rowerów, samochodów oraz wyznaczające strefy płatnego parkowania.

   Rozbudowane systemy monitoringu przestrzeni publicznej umożliwiające śledzenie osób i pozyskiwanie danych wykraczających poza dane niezbędne do świadczenia usługi.

2) Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki

   Systemy monitoringu wykorzystywane do zarządzania ruchem lub przeciwdziałania zagrożeniom/nadużyciom drogowym, umożliwiające szczegółowy nadzór nad każdym kierowcą oraz jego zachowaniem na drodze w szczególności systemy pozwalające na automatyczną identyfikację pojazdów.

   Drogi objęte odcinkowym pomiarem prędkości (system gromadzi informacje nie tylko o pojazdach naruszających przepisy, ale o wszystkich pojazdach pojawiających się w kontrolowanym obszarzej, odcinki dróg wyposażone w system elektronicznego poboru opłat viaTOLL.

Google Wajs Hubert Szukaj Szukanie zaawansowane

Szukaj w internecie Szukaj na stronach kategorii: język polski

Sieć Pokaż opcje... Wyniki **1** - **10** spośród około **24,500** dla zapytania **Wajs Hubert**. (Znaleziono w **0,21** sek.)

WAJS Hubert
Hubert Wajs (b. 1957) studied history, completing his doctorate in 1986, with a dissertation on the economy of medieval villages. Since 1983, he has worked ...
www.archiwa.gov.pl › ... › Prelegenci - Kopia - Podobne

Przechowywanie obiektów elektronicznych w długim czasie- dr **Hubert** ...
ArchNet ma przyjemność udostępnić szerokiemu odbiorcy, za zgodą autora, prezentację dr **Huberta Wajsa**, Dyrektora Archiwum Głównego Akt Dawnych pt: ...
www.archiwa.net/index.php?option...**hubert-wajs**... - Kopia

Archiwum Główne Akt Dawnych w Warszawie - strona główna
Dyrektor - dr **Hubert Wajs** ul. Długa 7, PL 00-263 Warszawa tel. (+ 48)(22) 831-54-91 do 93 fax. (+ 48)(22) 831-16-08 e-mail: sekretariat@agad.gov.pl ...
www.agad.archiwa.gov.pl/ - Kopia - Podobne

Niemiecki Institut Historyczny w Warszawie -- Results / Lista rekordów
Wajs, **Hubert**: Powinności feudalne chlopów na Mazowszu od XIV do początku XVI wieku: (w dobrach monarszych i kościelnych). - Ossolineum (1986) --- Sygnatura: ...
www.dhi.waw.pl/fileadmin/polkat/find.php?urG=%7C1...**wajs**,!**hubert**

[PDF] Inwentarz Metyki Koronnej w EAD
Format pliku: PDF/Adobe Acrobat - Szybki podgląd
HUBERT WAJS. Archiwum Główne Akt Dawnych. (Warszawa). Inwentarz Metryki Koronnej w EAD .... Kulecki, Inga Stembrowicz oraz **Hubert Wajs**. ...
karow.webpark.pl/13w.pdf - Podobne

Wyszukiwarka: wojewodztwa
77-86 Hubert Wajs Materialy skarbowe w aktach ziemskich i grodzkich w AGAD ... 87-96 Anna **Wajs**, **Hubert** Wajs Aneks, s. 97-115 Justyna Kliszewska Z badan nad ...
www.dig.com.pl/cgibin/search?words=wojewodztwa - Kopia

[PDF] pobierz PDF - NASK - ZMYSŁ TELEKOMUNIKACJI
Format pliku: PDF/Adobe Acrobat - Wersja HTML
Hubert Wajs. Dyrektor Archiwum Głównego Akt Dawnych. **Hubert Wajs** drogę do tego „wehikułu czasu" i dalej już można rozpocząć ...
www.nask.pl/biuletyn/biuletyn2004_03.pdf - Podobne

[PDF] (Dr M. Smoliński)
Format pliku: PDF/Adobe Acrobat - Wersja HTML
Wajs Hubert, Archiwa elektroniczne – problemy postępowania z ... **Wajs Hubert**, DLM-Forum poświęcone zagadnieniom dokumentów elektronicznych, Bruksela ...
www.historia.ug.gda.pl/upload/files/80/drmsmoliski.pdf - Podobne

Delos - Network of Excellence for Digital Libraries
30 Maj 2003 ... Mr **Hubert Wajs**, Dyrektor Naczelnego Archiwum Historycznego, Warszawa ....

Tytuł tematu: Konferencja "Zintegrowany System Informacji Archiwalnej ZoSIA", zorganizowana przez Narodowe Archiwum Cyfrowe w Warszawie

Opis obrazu: Uczestnicy konferencji podczas przerwy. Rozmowy kuluarowe. Od lewej: Hubert Wajs - dyrektor Archiwum Głównego Akt Dawnych i Eugeniusz Borodij - dyrektor Archiwum Państwowego w Bydgoszczy

Data wydarzenia: 2008-11-28

Miejsce: Warszawa

Osoby widoczne: Hubert Wajs, Eugeniusz Borodij,

Osoby niewidoczne:

Hasła przedmiotowe: archiwa, konferencje, uroczystości,

Inne nazwy własne: Archiwum Państwowe w Bydgoszczy, Narodowe Archiwum Cyfrowe, Archiwum Główne Akt Dawnych,

Zakład fotograficzny:

Autor: Nowak Rafał

Zespół: Zbiór fotografii dotyczących archiwów państwowych

Sygnatura: 31-182-11

myspace

Ludzie | Szukaj | POWERED BY Google

Zarejestruj się w MySpace

Adres e-mail:

Hasło:

Imię i nazwisko:

Data urodzenia: Dzień | Miesiąc | Rok

Płeć: Kobieta | Mężczyzna

Zapisz się

Wpisz adres e-mail
Wpisz prawidłowy adres e-mail. Musisz potwierdzić adres e-mail w celu uaktywnienia swojego konta.

Zaznaczając to pole, potwierdzasz, że wiesz o tym, że MySpace.com jest serwisem internetowym obsługiwanym przez firmę MySpace z siedzibą w Stanach Zjednoczonych, a także zgadzasz się na przesyłanie swoich danych osobowych do Stanów Zjednoczonych, gdzie będą podlegały przepisom prawa Stanów Zjednoczonych, określającym poziom ochrony danych w sposób inny niż stosowne przepisy w twoim kraju. Ponadto akceptujesz obowiązujący w MySpace Warunki użytkowania i dokument Polityka prywatności , które opisują sposób wykorzystywania danych osobowych.

Dlaczego warto zarejestrować się MySpace?

- Utrzymuj kontakty ze znajomymi i rodziną
- Udostępniaj albumy zdjęć i pliki wideo
- Znajdź starych znajomych ze szkoły i współpracowników
- Wszystko to BEZPŁATNIE.

Nie wysyłamy spamu. Doskonale wiemy w MySpace, że ochrona prywatności naszych użytkowników to klucz do naszego sukcesu. Oto nasza polityka prywatności.

Typy profili

Jeśli jesteś muzykiem, zapisz się tutaj!

Build and grow with Facebook Connect

On the Web | On the iPhone | On the Mobile Web

Connecting people everywhere.

Facebook Connect is a powerful set of APIs for developers that lets users bring their identity and connections everywhere. Developers can access a user's:

- **Identity:** name, photos, events, and more.
- **Social Graph:** friends and connections.
- **Stream:** activity, distribution, and integration points within Facebook, like stream stories and Publishers.

Use this information to create more engaging experiences on your website. Facebook Connect is free, so what are you waiting for? Be a part of making the Web more social and connecting people everywhere.

Start Building

- Want simple, powerful solutions with one line of code? Check out Facebook Widgets.
- Want to read the technical documentation? Visit our guides and documentation.
- See examples of great implementations.

What are the benefits of implementing Facebook Connect?

Facebook Connect delivers a number of benefits, including:

Traffic
Enable over 300 million Facebook users to share your content with their friends on Facebook. Let users publish a story, invite their friends, or send an event. Their friends then click back to your site.

Engagement
Users can immediately find their friends and engage. More friends leads to more activity and more pageviews. Connected users create 15-60% more content than users who have not connected with Facebook Connect.

Dodaj zdjęcie
Zrób zdjęcie

Edytuj profil

Twój progres:

Napisz coś o sobie

Informacje

Data urodzenia:
16 maja 1957

Znajomi

1 znajomy Pokaż wszystkich

Znajdź swoich znajomych

Monika Pol

Utwórz wizytówkę profilu

Hubert Wajs

Tablica | Informacje | +

Rzeczy, które Cię interesują, będą teraz widoczne w postaci linków do stron.
Dopasowaliśmy Twoje aktualne informacje z profilu do stron o danej tematyce.

Zobacz propozycje stron ▸

Edytuj informacje

Podstawowe informacje

Płeć: Mężczyzna
Data urodzenia: 16 maja 1957

Informacje kontaktowe

E-mail: hubert.wajs@gmail.com

Wykształcenie i praca

Szkoła wyższa: Uniwersytet Warszawski '80
Pracodawca: Archiwum Główne Akt Dawnych w Warszawie

Hubert Wajs
Samochody doszły już do ściany. Czas na drugą młodość kolei

Więcej... http://wyborcza.pl/1,75248,11492525,Samochody_doszly_juz_do_sciany__Czas_na_druga_mlodosc.html#ixzz1rEzIRdmx

> **Samochody doszły już do ściany. Czas na drugą młodość kolei**
> wyborcza.pl
> Ludzie chcą się przemieszczać coraz szybciej, a transport samochodowy osiągnął już limit możliwości. Musimy więcej korzystać z pociągów i samolotów - mówi Henri Poupart-Lafarge, prezes Alstom Transport

Lubię to! · Dodaj komentarz · Udostępnij · 6 kwietnia o 08:53 ·

Piotr Tafiłowski lubi to.

Hubert Wajs I znowu coś mnie 'pociaga', z 'kolei' do przewozów osobowych....
6 kwietnia o 08:54 · Lubię to!

Napisz komentarz...

Hubert Wajs
Tiry na Tory (http://www.tirynatory.pl/) to jest ważny problem; dlaczego np. w Austrii to się udaje, a tu - jak zwykle - jest inaczej.

> **Home**
> www.tirynatory.pl
> Jeden 40-tonowy TIR w ciągu 3 sekund rozjeżdża drogę jak 163 840 samochodów osobowych, przejeżdżających przez ten sam punkt.

Lubię to! · Dodaj komentarz · Udostępnij · 5 kwietnia o 18:45 ·

Piotr Tafiłowski lubi to.

Napisz komentarz...

Hubert Wajs

Sportu Michał...

+

udio Tańca i Piosenki "Szachraj"
członków

ago Turci - The Image of the Turk
4 członków
e are forming a group to improve...

Wajs · ponad rok temu

eż przypomnieć sobie dokonania
wieku i wyobrazić, jakie konsekwencje
ąć za sobą ich bezmyślne odrzucenie.
ekscytująco niż planowanie wielkich

Lubię to! · Dodaj komentarz · Udostępnij

Rejestracja i bezpieczeństwo konta

- Użytkownicy serwisu Facebook podają swoje prawdziwe imiona i nazwiska oraz dane. Potrzebujemy pomocy użytkowników, aby utrzymać ten stan rzeczy. Poniżej zawarto przyjęte przez użytkownika zobowiązania względem serwisu Facebook, które dotyczą rejestracji oraz troski o bezpieczeństwo konta:
- 1. Zabronione jest podawanie fałszywych danych osobowych na Facebooku i tworzenie konta dla innej osoby bez jej pozwolenia.
- 2. Użytkownik może utworzyć tylko jedno konto osobiste.
- 3. W przypadku zablokowania konta użytkownik nie ma prawa utworzyć kolejnego bez naszego zezwolenia.
- 4. Zabronione jest wykorzystywanie osobistej osi czasu głównie do celów komercyjnych. Do takich zastosowań są przeznaczone strony na Facebooku.
- 5. Zabronione jest korzystanie z Facebooka przez osoby poniżej 13. roku życia.

Dziecko pozostaje pod opieką rodzica (lub opiekuna) aż do uzyskania pełnoletności. Rodzice są przedstawicielami ustawowymi swojego nieletniego dziecka i to oni odpowiedzialni są za zachowanie się małoletniego.
Co do zasady małoletni który nie ukończył 13 roku życia nie ponosi za wyrządzone przez siebie szkody. Nie oznacza to jednak, że poszkodowany nie może w takim przypadku, domagać się odszkodowania. Za szkody wyrządzone przez dzieci odpowiadają rodzice lub ich prawni opiekunowie, gdyż ten który, z mocy ustawy lub umowy, jest obowiązany do nadzoru nad osobą która z powodu wieku nie może odpowiadać za swoje czyny, zobowiązany jest do naprawienia szkody wyrządzonej przez tę osobę.

* * *

KC Art. 426. **Małoletni, który nie ukończył lat trzynastu, nie ponosi odpowiedzialności za wyrządzoną szkodę**.

AGAD 2020 na FB

*Znowu ktoś mnie **podgląda**,*
Lekko skrobie do drzwi.
Strasznym okiem cyklopa,
Radzi, gromi i drwi!

Mój jest ten kawałek podłogi,
Nie mówcie mi więc, co mam robić!

Mr. Zoob

Archiwum Główne Akt Dawnych
@AGAD.Warszawa

Strona główna
Informacje
Zdjęcia
Notatki
Recenzje
Filmy
Wydarzenia
Posty
Usługi
Sklep
Oferty
Oferty pracy
Społeczność

Lubisz to! | Obserwowanie | Udostępnij | ...

+ Dodaj przycisk

Pokaż wszystkie

Notatki Zobacz wszystkie

„Siedlce się stały rozkoszy rajem, ty raju tego ozdobą" – opis zabaw urządzanych w 1786 r. przez Aleksandrę Ogińską

27 stycznia

Aleksandra Czartoryska urodziła się w 1730 roku. Była córką Michała Fryderyka Czartoryskiego, kanclerza wielkiego litewskiego i El...

Pobierz Menedżera stron, aby publikować posty i odpowiadać gościom strony, kiedy jesteś w ruchu.

Utwórz grupę do swojej strony
Pomóż odbiorcom łączyć się ze sobą w grupie. Grupy to oddzielne przestrzenie do prowadzenia dyskusji, planowania wydarzeń, udostępniania zdjęć i filmów itd. Możesz prowadzić interakcję z członkami grupy osobiście lub jako swoja strona.

Zobacz wszystkie wskazówki dotyczące stron 1

Wskaźnik odpowiedzi 60%, czas odpowiedzi 38 min
Odpowiadaj szybciej, aby zdobyć oznaczenie

8557 obserwujących

251 osób było tutaj 0 w tym tygodniu

Zobacz aktualności ze stron
Posty ze stron, które lubisz jako swoja strona

Post dotarł do 3041 osób w tym tygodniu

10 wyświetleń filmu w tym tygodniu

Plik Edycja Widok Narzędzia Wiadomość Pomoc

Odpowiedz | Odpowiedz wszystkim | Prześlij dalej

Od: Facebook <notification+zj4ozs2t62zc@facebookmail.com>;
Data: 29 listopada 2011 14:28
Do: Hubert Wajs <hubert.wajs@gmail.com>;
Temat: Twoja cotygodniowa informacja na temat strony na Facebooku:

facebook

Witaj Hubert!

Oto tygodniowe zestawienie dla Twojej strony na Facebooku:

Archiwum Główne Akt Dawnych

Liczba aktywnych użytkowników w miesiącu: 505 ⬆ 27 od zeszłego tygodnia

Liczba osób, które to lubią: 479 . ⬆ 10 od zeszłego tygodnia

Liczba postów na tablicy i komentarzy w tym tygodniu: 16 ⬇ 19 od zeszłego tygodnia

Liczba odwiedzin w tym tygodniu: 305 ⬆ 65 od zeszłego tygodnia

- Prześlij aktualizację osobom, które lubią stronę
- Odwiedź swoją stronę statystyk
- Promuj się za pomocą reklamy na Facebooku

Dowiedz się więcej o aktualizacji przez telefon komórkowy

Dziękujemy
Zespół Facebooka

Od: Facebook <notification+zj4ozs2t62zc@facebookmail.com>;
Data: 6 grudnia 2011 08:13
Do: Hubert Wajs <hubert.wajs@gmail.com>;
Temat: Twoja cotygodniowa informacja na temat strony na Facebooku:

facebook

Witaj Hubert!

Oto tygodniowe zestawienie dla Twojej strony na Facebooku:

Archiwum Główne Akt Dawnych

Liczba aktywnych użytkowników w miesiącu: 490 ↓ 15 od zeszłego tygodnia

Liczba osób, które to lubią: 482 . ↑ 3 od zeszłego tygodnia

Liczba postów na tablicy i komentarzy w tym tygodniu: 17 ↑ 0 od zeszłego tygodnia

Liczba odwiedzin w tym tygodniu: 304 ↓ 1 od zeszłego tygodnia

- Prześlij aktualizację osobom, które lubią stronę
- Odwiedź swoją stronę statystyk
- Promuj się za pomocą reklamy na Facebooku

Dowiedz się więcej o aktualizacji przez telefon komórkowy

Dziękujemy
Zespół Facebooka

Data: 13 grudnia 2011 21:49

Do: Hubert Wajs <hubert.wajs@gmail.com>;

Temat: Twoja cotygodniowa informacja na temat strony na Facebooku:

facebook

Witaj Hubert!

Oto tygodniowe zestawienie dla Twojej strony na Facebooku:

Archiwum Główne Akt Dawnych

Liczba aktywnych użytkowników w miesiącu: 492 ⬆ 2 od zeszłego tygodnia

Liczba osób, które to lubią: 485 . ⬆ 3 od zeszłego tygodnia

Liczba postów na tablicy i komentarzy w tym tygodniu: 11 ⬇ 6 od zeszłego tygodnia

Liczba odwiedzin w tym tygodniu: 208 ⬇ 96 od zeszłego tygodnia

- Prześlij aktualizację osobom, które lubią stronę
- Odwiedź swoją stronę statystyk
- Promuj się za pomocą reklamy na Facebooku

Dowiedz się więcej o aktualizacji przez telefon komórkowy

Dziękujemy
Zespół Facebooka

Statystyki › Archiwum Główne Akt Dawnych › Użytkownicy

+ Utwórz reklamę

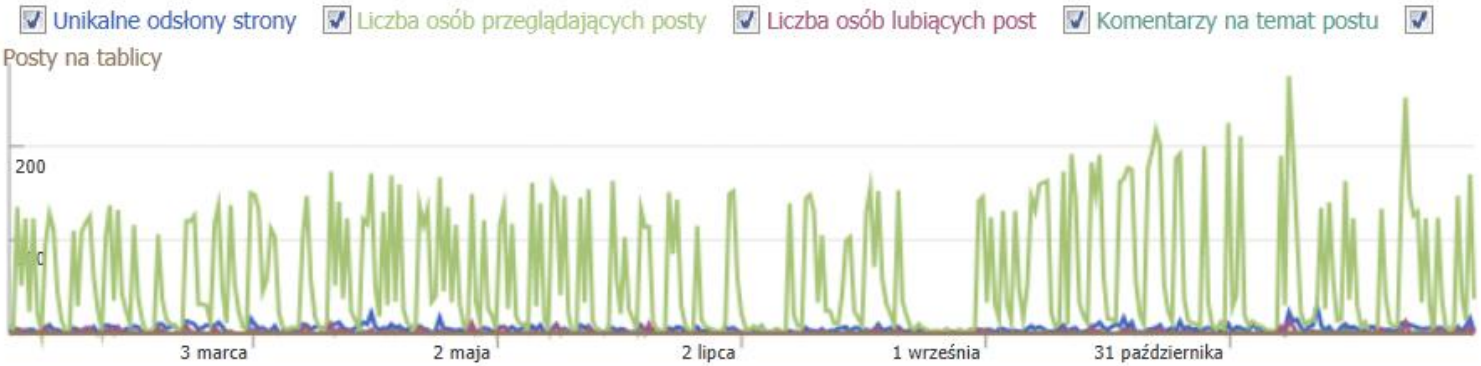
Tydzień | Miesiąc | 2011-01-01 – 2011-12-31

Nowe znaczniki „Lubię to”[?]
301 ↑12%

Znaczników „Lubię to” od początku[?]
499

Aktywni Użytkownicy[?]

Rozkład Liczba aktywnych użytkowników dziennie[?]



Archiwum Główne Ak...

Statystyki strony
- Przegląd
- Użytkownicy
- Interakcje

Linki
- Idź do strony
- Dokumentacja
- Wyślij opinię

W dn. 15 grudnia 2011 to narzędzie przestanie gromadzić dane. Wszystkie Twoje dane są już gromadzone w ramach nowych Statystyk strony. Wszystkie informacje z tej strony zostaną usunięte w dn. 15 lutego 2012 - wyeksportuj wszystkie dane, które chcesz zachować.

Rozpocznij korzystanie z nowych narzędzi Statystyk strony już dziś.

Statystyki › Archiwum Główne Akt Dawnych › Użytkownicy

+ Utwórz reklamę

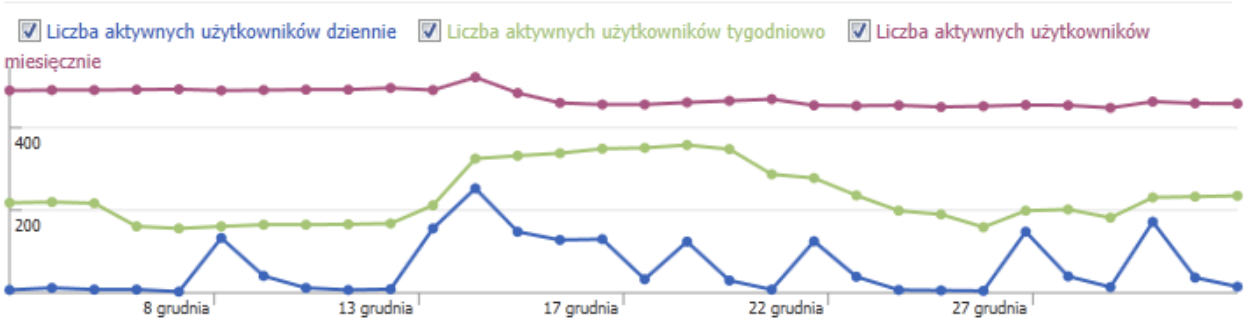
Tydzień | Miesiąc | 2011-12-03 – 2012-01-01

Nowe znaczniki „Lubię to”? **22** ↓29%

Znaczników „Lubię to” od początku? **499**

Liczba aktywnych użytkowników miesięcznie? **458** ↓10%

Aktywni Użytkownicy?



Rozkład Liczba aktywnych użytkowników dziennie?

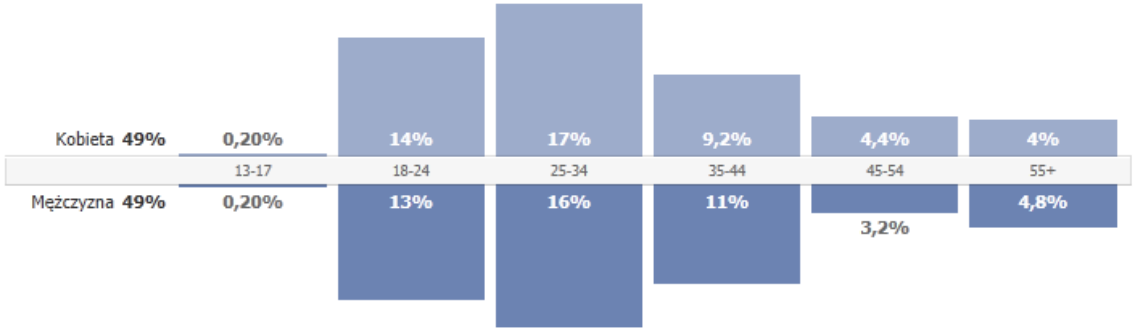
Nowe znaczniki „Lubię to”? Dziennie Łącznie

Źródła "Lubię to"?

20 Nieznana
1 Propozycje
1 Profil użytkownika

Dane demograficzne

Płeć i wiek?



Kraje?

429 Polska
10 Niemcy
8 Wielka Brytania
7 Stany Zjednoczone
5 Republika Czeska
4 Białoruś
4 Ukraina
Więcej

Miasta?

177 Warsaw
25 Lublin
23 Poznan
18 Krakow
15 Torun
13 Wroclaw

Język?

426 polski
25 Angielski (Amerykański)
14 Angielski (Wielka Brytania)
7 Niemiecki
4 Czeski
3 Białoruski
3 Francuski (Francja)
Więcej

Aktywność

Wyświetlenia strony?

Wyświetlenia strony Unikalne odsłony strony

Kraje[?]

429	Polska
10	Niemcy
8	Wielka Brytania
7	Stany Zjednoczone
5	Republika Czeska
4	Białoruś
4	Ukraina
3	Francja
3	Hiszpania
3	Irlandia
3	Litwa
3	Izrael
2	Holandia
2	Grecja
2	Włochy
1	Australia
1	Bangladesh
1	Korea Południowa
1	Norwegia

Zwiń

Miasta[?]

177	Warsaw
25	Lublin
23	Poznan
18	Krakow
15	Torun
13	Wroclaw

Język[?]

426	polski
25	Angielski (Amerykański)
14	Angielski (Wielka Brytania)
7	Niemiecki
4	Czeski
3	Białoruski
3	Francuski (Francja)
2	Hiszpański
2	Grecki
2	Ukraiński
2	Włoski
1	Hiszpański (Hiszpania)
1	Koreański
1	Litewski
1	Rosyjski
1	Szwedzki
1	Turecki

Zwiń

Aktywność

Wyświetlenia strony[?]

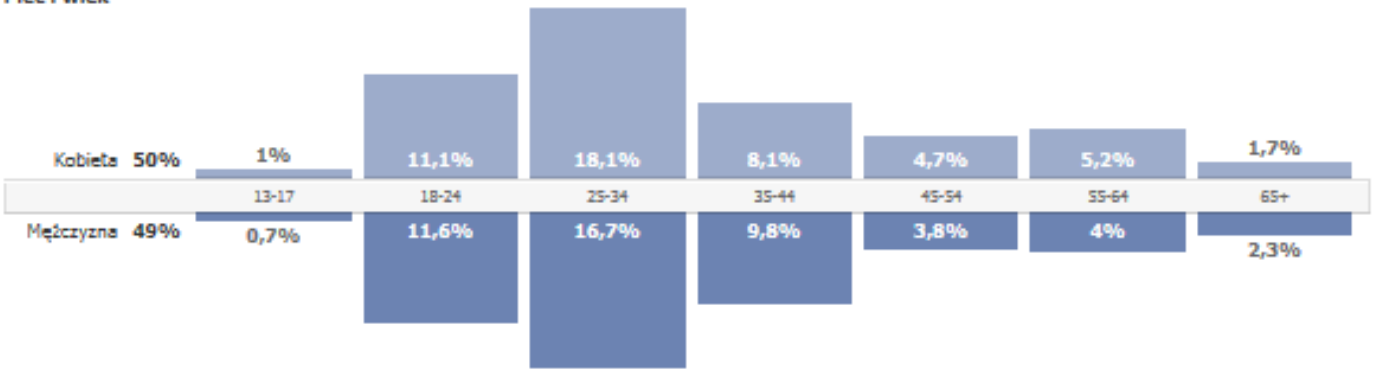
☑ Wyświetlenia strony ☑ Unikalne odsłony strony

Przegląd | Kliknięcia „Lubię to" | Zasięg | Liczba osób, które o tym mówią

2012-11-01 – 2013-01-16 | Eksportuj dane

Osoby, do których udało Ci się dotrzeć (Dane demograficzne i lokalizacja)

Płeć i wiek[7]



Kraje[7]

1.565	Polska
65	Ukraina
45	Niemcy
34	Stany Zjednoczone
25	Wielka Brytania
21	Senegal
19	Rosja
14	Francja
12	Kanada
10	Białoruś
10	Ghana
8	Włochy
8	Belgia
7	Szwecja
6	Irlandia
5	Brazylia
5	Republika Czeska
5	Izrael
5	Litwa
5	Holandia

Miasta[7]

456	Warsaw, Warszawa
73	Lublin, Lubelskie
64	Torun, Torun
57	Poznan, Wielkopolskie
49	Wroclaw, Wroclaw
43	Opole, Opolskie
36	Lviv, L'vivs'ka Oblast'
24	Pruszków, Warszawa
21	Kraków, Malopolskie
19	Łódź, Lodz
18	Gdansk, Pomorskie
16	Bydgoszcz, Kujawsko-Pomorskie
15	Gdynia, Gdansk
14	Dakar, Dakar
14	Kyiv, Kyyivs'ka Oblast'
12	Mokotów, Warszawa
11	Olsztyn, Warminsko-Mazurskie
11	Szczecin, Zachodniopomorskie
11	Katowice, Slaskie
11	Bialystok, Bialystok

Języki[7]

1.554	Polski
121	Angielski (Amerykański)
58	Francuski (Francja)
40	Angielski (Wielka Brytania)
37	Ukraiński
35	Rosyjski
33	Niemiecki
7	Włoski
4	Hiszpański
4	Czeski
3	Szwedzki
3	Arabski
3	Portugalski (Brazylia)
3	Chorwacki
3	Litewski
3	Białoruski
2	Hiszpański (Hiszpania)
2	Bułgarski
1	Słoweński
1	Japoński

Wskaźniki wzorcowe
Porównanie średnich wyników w czasie

- Oś czasu
- Karta Zdjęcia
- Karta Informacje
- Karta administratora
- Inne

Inna aktywność na stronie

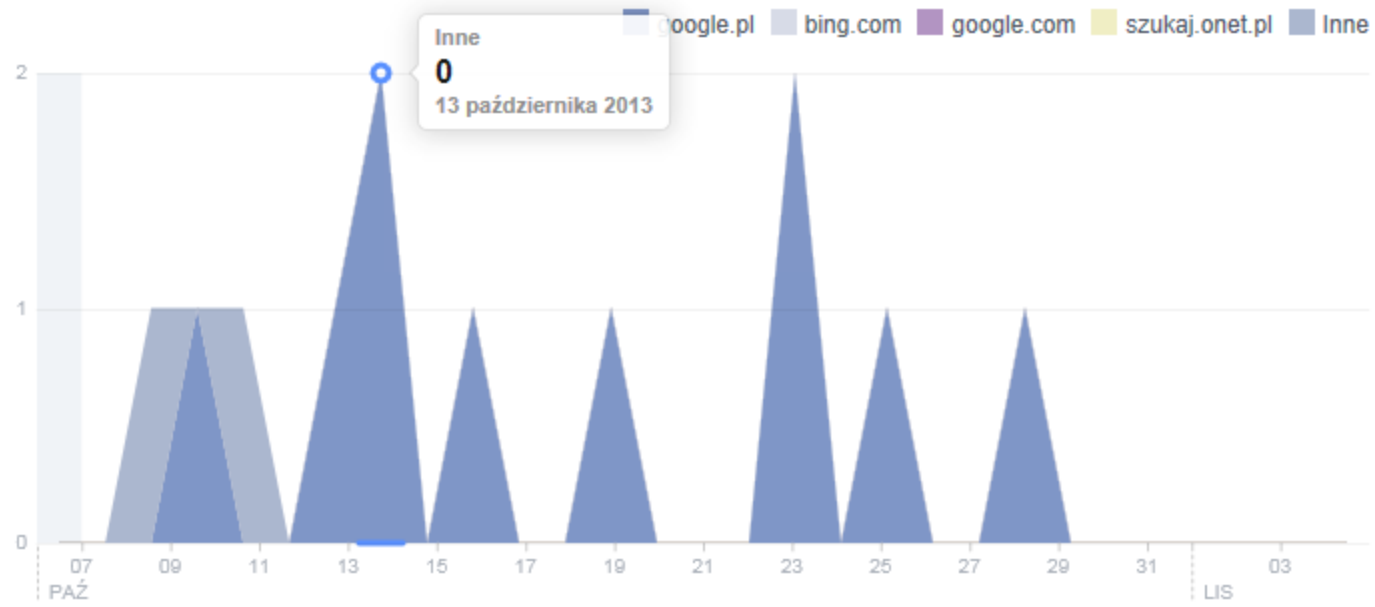
Liczba podjętych działań, które dotyczyły strony.

Wskaźniki wzorcowe
Porównanie średnich wyników w czasie

- Wzmianki
- Posty innych osób na T...
- Zameldowania
- Wykupione oferty

Źródła zewnętrzne

Liczba odwiedzin na stronie pochodzących z witryn poza serwisem Facebook.



Wskaźniki wzorcowe

Porównanie średnich wyników w czasie

- google.pl
- bing.com
- google.com
- szukaj.onet.pl
- Inne

Archiwum Główne Akt Da... Oś czasu Najnowsze Panel administratora

Archiwum Główne Akt Dawnych

1.705 osób lubi to · 74 osoby o tym mówią
· 5 were here

Zaktualizuj informacje o stronie ✓ Lubisz to!

Usługi publiczne
Długa 7, 00-263 Warsaw, Poland
(+ 48)(22) 831-54-91 do 93
Następne otwarcie: Czwartek 09:00 - 19:00

Informacje

Zdjęcia

1.705

Osoby, które to lubią

Mapa

Filmy

1

Wyróżnione

Archiwum Główne Akt Dawnych

Hubert | Strona główna | Szukaj znajomych

Strona | Skrzynka odbiorcza | Powiadomienia 1 | Statystyki | Narzędzia do publikowania

Archiwum Główne Akt Dawnych

@AGAD.Warszawa

Strona główna

Informacje

Lubisz to! | Obserwowanie | Udostępnij | ···

Wyniki z okresu **9 lutego 2018 – 15 lutego 2018**
Uwaga: dzisiejsze dane nie są uwzględnione. Aktywność w statystykach jest raportowana z czasem pacyficznym.
Aktywność w reklamach jest raportowana z czasem strefy przypisanej do konta reklamowego.

Organiczne Płatne

Działania na stronie
8 lutego – 14 lutego

Brak danych z tego tygodnia.

Liczba wyświetleń strony
8 lutego – 14 lutego

166

Łączna liczba wyświetleń strony ▼39%

Wyświetlenia podglądu strony
8 lutego – 14 lutego

32

Wyświetlenia podglądu strony ▼53%

Polubienia strony
8 lutego – 14 lutego

4

Polubienia strony ▼80%

Zasięg
8 lutego – 14 lutego

3397

Liczba odbiorców ▼55%

Rekomendacje
8 lutego – 14 lutego

Brak danych z tego tygodnia.

Aktywność dotycząca postów
8 lutego – 14 lutego

592

Aktywność dotycząca postów ▼33%

Filmy
8 lutego – 14 lutego

2

Łączna liczba wyświetleń filmu ▼71%

Osoby obserwujące stronę
8 lutego – 14 lutego

5

Osoby obserwujące stronę ▼77%

Podsumowanie
Reklamy
Osoby obserwujące
Polubienia
Zasięg
Wyświetlenia strony
Wyświetlenia podglądu strony
Działania na stronie
Posty
Wydarzenia
Filmy
Zdarzenia
Osoby
Wiadomości
Zamówienia

Aktywność w reklamach jest raportowana z czasem strefy przypisanej do konta reklamowego.

Działania na stronie
15 lutego–21 lutego

Mamy niewystarczające dane, aby wyświetlić je dla wybranego okresu.

Liczba wyświetleń strony
15 lutego–21 lutego

213

Łączna liczba wyświetleń strony ▲9%

Wyświetlenia podglądu strony
15 lutego–21 lutego

29

Wyświetlenia podglądu strony ▲16%

Polubienia strony
15 lutego–21 lutego

12

Polubienia strony ▼20%

Zasięg posta
15 lutego–21 lutego

5,237

Liczba odbiorców ▼22%

Zasięg relacji
15 lutego–21 lutego

Uzyskaj statystyki relacji

Zobacz statystyki wyników ostatnich relacji strony.

Dowiedz się więcej

Rekomendacje
15 lutego–21 lutego

Mamy niewystarczające dane, aby wyświetlić je dla wybranego okresu.

Aktywność dotycząca posta
15 lutego–21 lutego

1,101

Aktywność dotycząca posta ▲2%

Szybkość udzielania odpowiedzi
Stan na dzień: 20 lutego 2020

60%

Wskaźnik odpowiedzi ▲0%

0 godz. 38 min

Czas odpowiedzi ▲0 godz. 0 min

Filmy
15 lutego–21 lutego

10

3-sekundowe wyświetlenia filmu ▲25%

Osoby obserwujące stronę
15 lutego–21 lutego

13

Osoby obserwujące stronę ▼19%

Zamówienia
15 lutego–21 lutego

0

Liczba zamówień ▲0%

Opublikowane posty

+ Utwórz

Szukaj... Działania

Posty	Zasięg	Kliknięcia/działania	Opublikowane
	506	31	16 lutego 2018 o 10:04 Rafał Górny
„Gdy rozumieli, że skonał, ruszyli poduszki a on im parę fig ukazał"	2261	94	9 lutego 2018 o 10:47 Karol Zgliński
 Archiwum Główne Akt Dawnych udostępnił(a) post użytkownika Archiwa	2149	126	8 lutego 2018 o 19:00 Karol Zgliński
Archiwum Główne Akt Dawnych udostępnił(a) link.	2063	146	8 lutego 2018 o 09:01 Karol Zgliński
 Archiwum Główne Akt Dawnych udostępnił(a) post użytkownika More	1353	24	7 lutego 2018 o 04:56 Karol Zgliński
„Podlaskie Rivendell" – historyczna kraina na styku dokumentów	7240	511	2 lutego 2018 o 10:29 Karol Zgliński
Listy Benedykta Dybowskiego pisane do Władysława Taczanowskiego z Syberii	1737	47	30 stycznia 2018 o 09:46 Karol Zgliński
„Wiarygodność moja nigdy w niczym nie była poszlakowana" – reprotestacja	1528	54	29 stycznia 2018 o 08:49 Karol Zgliński
 Papieski Instytut Studiów Kościelnych w Rzymie to instytucja, która zajmuje się	1458	54	26 stycznia 2018 o 11:04 Rafał Górny
 W związku z tym, że awaria w serwisie szukajwarchiwach.pl została	2357	141	24 stycznia 2018 o 08:16 Rafał Górny
https://www.nac.gov.pl/brakujace-skany-w-serwisie-szukaj-w-archiwach/	1728	93	24 stycznia 2018 o 08:07 Karol Zgliński

MOST POPULAR WEBSITES

Today's Most Popular Websites on the Internet:
Friday, November 1st 2013

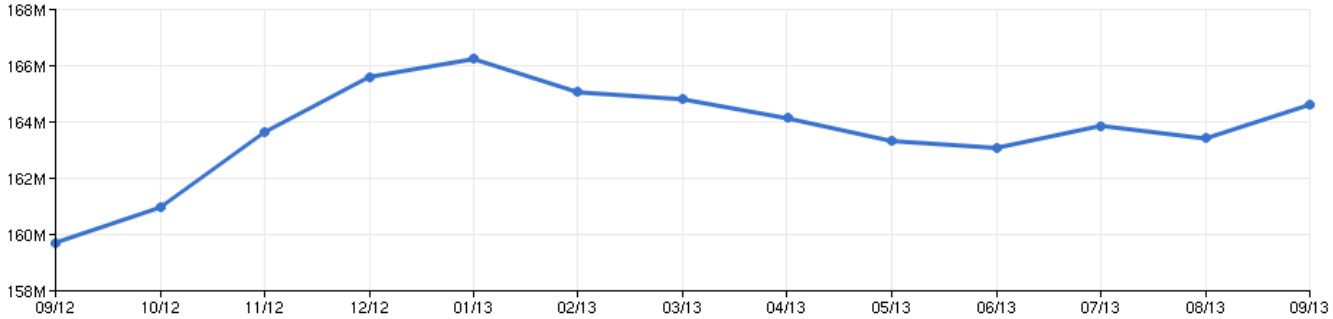
NEW! Website Lists | Winners | Losers | Top Level Domains | Webmasters

#	Website:	Report:	Last Wk.	Chang
1.	Google.com	www.google.com	1	=
2.	Facebook.com	www.facebook.com	2	=
3.	Youtube.com	www.youtube.com	3	=
4.	Yahoo.com	www.yahoo.com	4	=
5.	Baidu.com	www.baidu.com	5	=
6.	Wikipedia.org	www.wikipedia.org	6	=
7.	Qq.com	www.qq.com	7	=
8.	Linkedin.com	www.linkedin.com	8	=
9.	Windows Live	www.live.com	10	↑
10.	Twitter.com	www.twitter.com	9	↓
11.	Amazon.com	www.amazon.com	11	=
12.	Blogger	www.blogspot.com	12	=
13.	Taobao.com	www.taobao.com	13	=

Facebook.com Is Worth an Estimated Value of 2.41 Billion

Estimated Daily Ad Revenue: 3300003.16

UVs for facebook.com

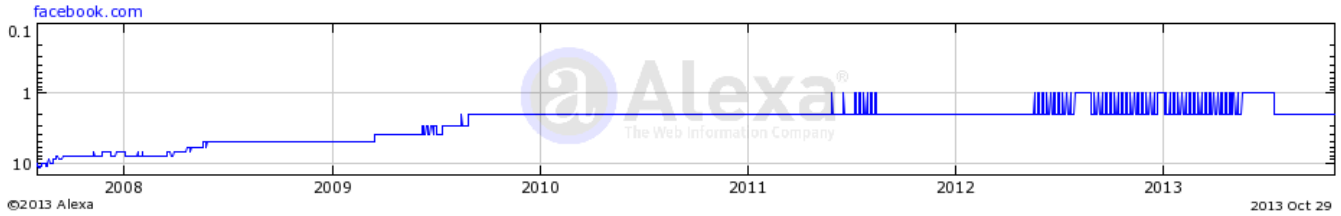


compete
www.compete.com

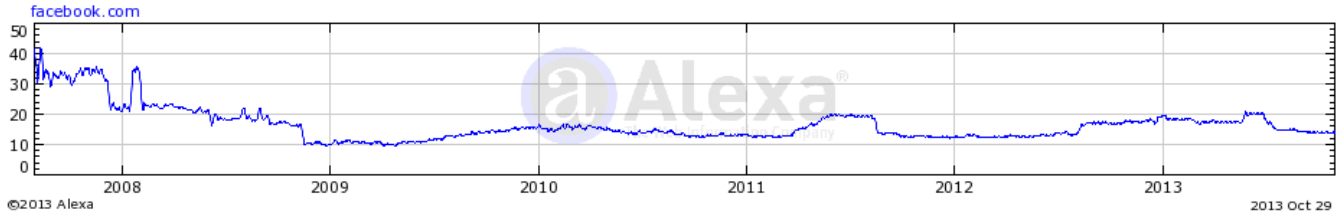
Facebook.com Stock Market Data: (Ticker Symbol: FB)

Alexa Graphs for www.facebook.com

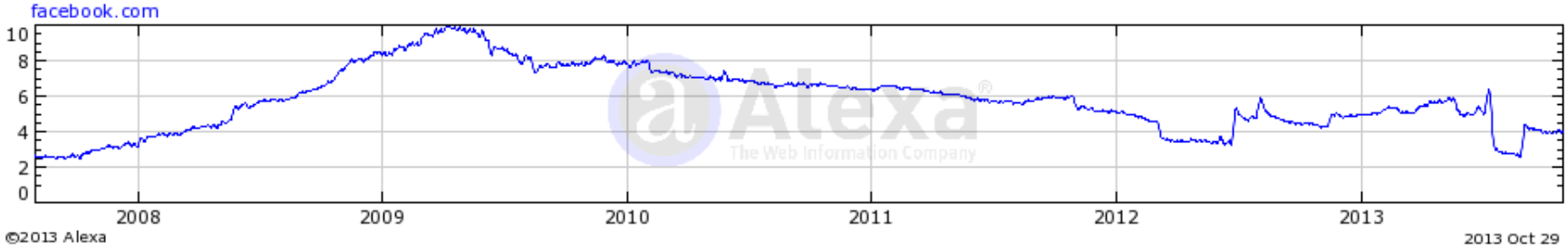
facebook.com Popularity & Rank History:



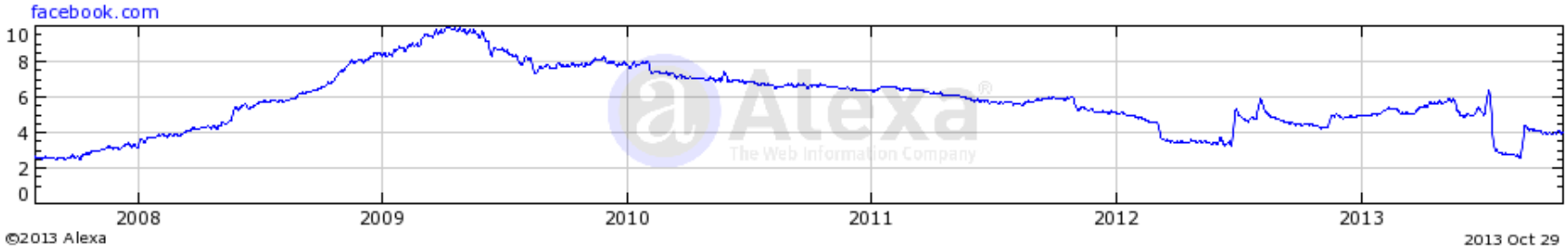
Average Number of Pages Viewed by Most Visitors on www.facebook.com:



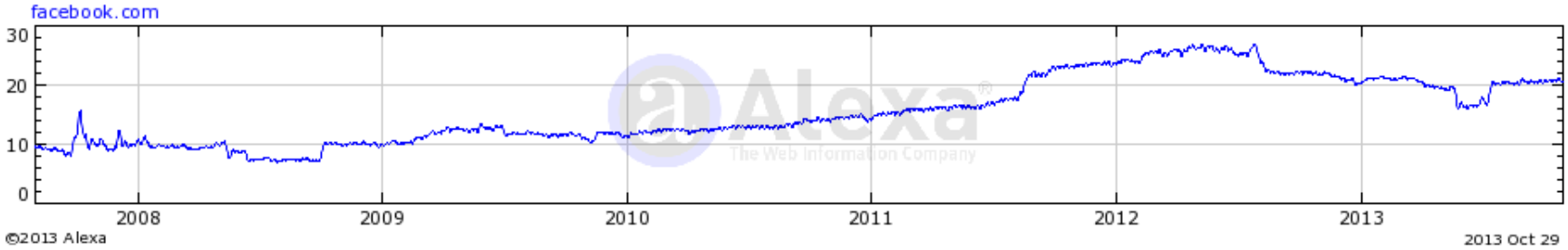
Percentage of facebook.com Traffic Coming from Search Engines:



Avg. Time Spent on www.facebook.com:



facebook.com Bounce Rate:



www.facebook.com News:

Technologia G

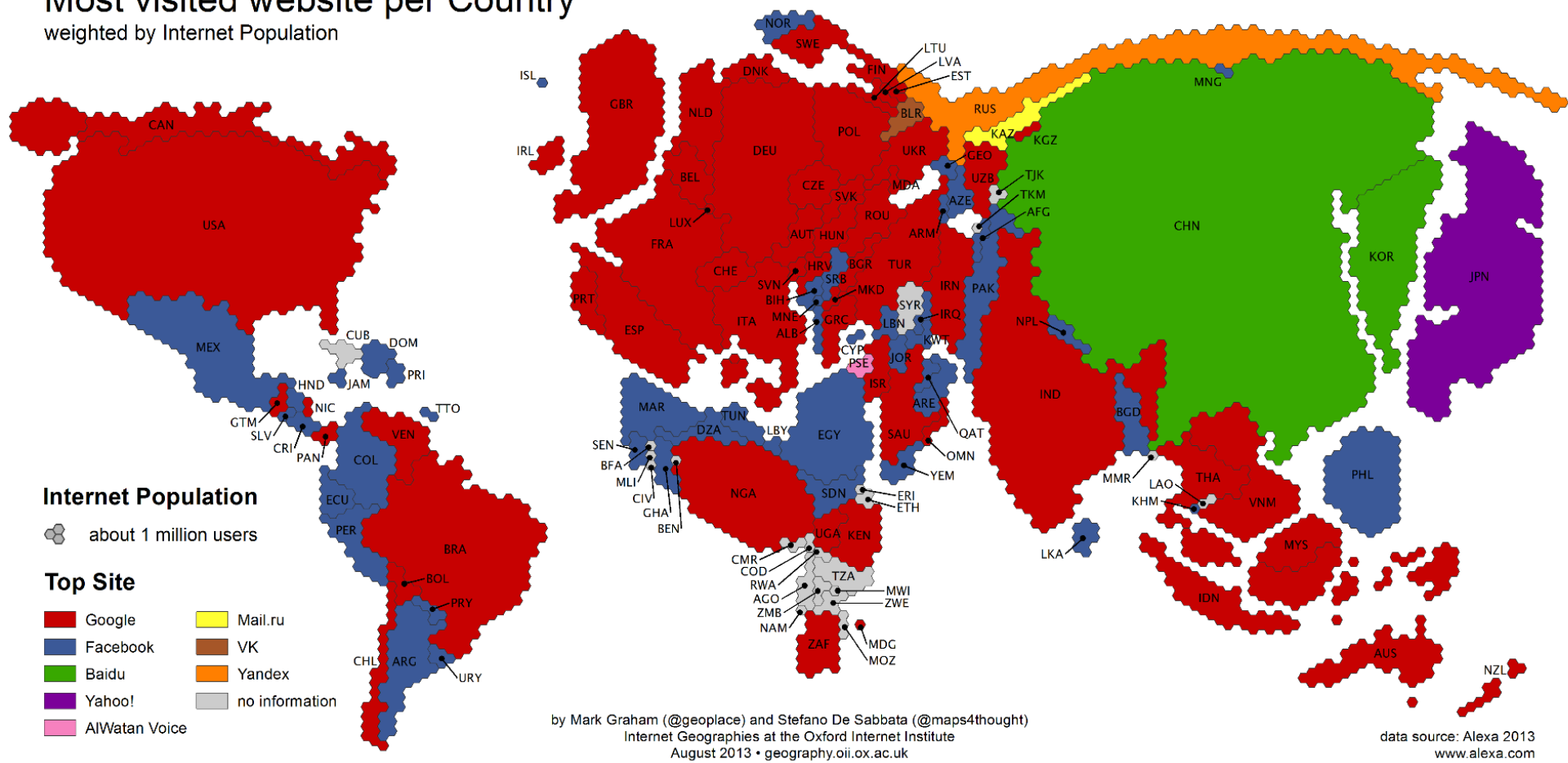
What **Facebook** should say to Forrester

Facebook (ticker: FB) seems to be having the last laugh after posting blowout quarterly results yesterday. Earlier in the week, tech research advisory firm Forrester Research had called out the world's largest social networking website in an open **...**

USA TODAY Fri, 01 Nov 2013 09:52:30 -0700

Most visited website per Country

weighted by Internet Population



Internet Population

about 1 million users

Top Site

- Google
- Facebook
- Baidu
- Yahoo!
- AlWatan Voice
- Mail.ru
- VK
- Yandex
- no information

by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
August 2013 • geography.oii.ox.ac.uk

data source: Alexa 2013
www.alexa.com


SURVEILLANCE

chitect Paul Van Welden Komentarze Prześlij zdjecia

aul Van Welden - Zgłoś problem

USTAWA z dnia 15 stycznia 2016 r. **o zmianie ustawy o Policji oraz niektórych innych ustaw**

- Warszawa, dnia 4 lutego 2016 r., Dz. U., Poz. 147
- Sejm uchwalił ustawę 15 stycznia 2016 r. Prezydent podpisał ją 3 lutego br. Zmienione przepisy obowiązują od 7 lutego 2016 r.

- **Art. 1.** W ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 r. poz. 355, z późn. zm.2)) wprowadza się następujące zmiany:

Zmiany w zasadach prowadzenia kontroli operacyjnej przez służby

- Nowelizacja ustawy o Policji oraz niektórych innych ustaw doprecyzowuje zasady stosowania kontroli operacyjnej przez służby mundurowe. Ustawa dostosowuje przepisy do wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. Zmienione przepisy dotyczą działań prowadzonych przez:
- Policję,
- organy kontroli skarbowej,
- Straż Graniczną,
- Żandarmerię Wojskową,
- Agencję Bezpieczeństwa Wewnętrznego,
- Agencję Wywiadu,
- Służbę Kontrwywiadu Wojskowego,
- Służbę Wywiadu Wojskowego,
- Centralne Biuro Antykorupcyjne i
- Służbę Celną.

Zmiany w zasadach prowadzenia kontroli operacyjnej przez służby

- Dokument precyzuje środki i metody, za pomocą których będzie możliwe prowadzenie w sposób niejawny kontroli operacyjnej. Są to czynności podejmowane przez służby mundurowe w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, wymienionych w ustawie poważnych przestępstw. Wśród czynności zaliczonych do kontroli operacyjnej nowelizacja wymienia uzyskiwanie i utrwalanie treści rozmów, obrazu i dźwięku, treści korespondencji, w tym prowadzonej elektronicznie, danych zawartych w systemach informatycznych i teleinformatycznych oraz kontrolę zawartości przesyłek.
- Kontrola operacyjna będzie tak jak dotychczas zarządzana przez sąd okręgowy na wniosek skierowany przez właściwą służbę. Zgodnie z ustawą kontrola operacyjna będzie mogła być prowadzona maksymalnie przez 18 miesięcy.
- Ustawa porządkuje też katalog danych, które będą mogły być pozyskiwane przez służby w celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych. Zgodnie z nowelizacją będzie to możliwe w odniesieniu do niestanowiących treści danych telekomunikacyjnych, pocztowych i internetowych. Ponadto ustawa określa procedury weryfikacji i niszczenia danych zbędnych dla prowadzonego postępowania – mają one podlegać niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu.
- Ustawa określa też zasady postępowania z materiałami, które mogą zawierać informacje objęte tajemnicą zawodową. Dane zawierające tajemnice obrończe i spowiedzi będą natychmiast niszczone. W przypadku danych stanowiących inne tajemnice zawodowe – m.in. lekarską, dziennikarską i statystyczną – o ich wykorzystaniu lub zniszczeniu ma decydować sąd, kierując się dobrem wymiaru sprawiedliwości oraz tym, czy dana okoliczność może być ustalona na podstawie innego dowodu.
- Przedsiębiorcy telekomunikacyjni, operatorzy pocztowi oraz firmy świadczące usługi drogą elektroniczną będą zobowiązani do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie kontroli. W przypadku mikro i małych przedsiębiorców świadczących usługi drogą elektroniczną, obowiązek ten będzie ograniczony do możliwości wynikających z posiadanej przez nich infrastruktury.
- W celu zapewnienia opinii publicznej niezbędnych informacji ustawa nakłada na ministra sprawiedliwości obowiązek przedstawiania Sejmowi i Senatowi corocznej informacji na temat przetwarzania danych oraz wyników przeprowadzonych kontroli. Termin na jej przedstawienie Izba określiła na 30 czerwca.

- 6. Kontrola operacyjna prowadzona jest niejawnie i polega na:
- 1) uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych;
- 2) uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne;
- 3) uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej;
- 4) uzyskiwaniu i utrwalaniu **danych zawartych w informatycznych nośnikach danych**, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;
- 5) uzyskiwaniu dostępu i kontroli zawartości przesyłek.

- Sąd okręgowy, Prokurator Generalny, prokurator okręgowy i organ Policji prowadzą rejestry postanowień, pisemnych zgód, wniosków i zarządzeń dotyczących kontroli operacyjnej.
- 16b. Komendant Główny Policji prowadzi rejestr centralny wniosków i zarządzeń dotyczących kontroli operacyjnej prowadzonej przez organy Policji w zakresie przewidzianym dla prowadzonych przez nie rejestrów.
- 16c. W komórkach organizacyjnych Policji wykonujących zarządzenia w sprawie kontroli operacyjnej można odrębnie rejestrować dane zawarte w dokumentacji z kontroli operacyjnej w zakresie przewidzianym dla prowadzonych przez organy Policji rejestrów, o których mowa w ust. 16a.
- 16d. Rejestry, o których mowa w ust. 16a–16c, prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.”,

- „Art. 20ca. 1. Kontrolę nad uzyskiwaniem przez Policję danych telekomunikacyjnych, pocztowych lub internetowych sprawuje sąd okręgowy właściwy dla siedziby organu Policji, któremu udostępniono te dane.
- 2. Organ Policji, o którym mowa w ust. 1, przekazuje, z zachowaniem przepisów o ochronie informacji niejawnych, sądowi okręgowemu, o którym mowa w ust. 1, w okresach półrocznych, sprawozdanie obejmujące:
  - 1) liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych;
  - 2) kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe, albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.
- 3. W ramach kontroli, o której mowa w ust. 1, sąd okręgowy może zapoznać się z materiałami uzasadniającymi udostępnienie Policji danych telekomunikacyjnych, pocztowych lub internetowych.
- 4. Sąd okręgowy informuje organ Policji o wyniku kontroli w terminie 30 dni od jej zakończenia.
- 5. Kontroli, o której mowa w ust. 1, nie podlega uzyskiwanie danych na podstawie art. 20cb ust. 1.

- „Art. 20c. 1. W celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Policja może uzyskiwać dane **niestanowiące** treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:
  - 1) art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.4)), zwane dalej „danymi telekomunikacyjnymi”,
  - 2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529 oraz z 2015 r. poz. 1830), zwane dalej „danymi pocztowymi”,
  - 3) art. 18 ust. 1–5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422 oraz z 2015 r. poz. 1844), zwane dalej „danymi internetowymi”
- – oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

- po art. 175a dodaje się art. 175b w brzmieniu:
- „Art. 175b. § 1. Prezesi sądów okręgowych właściwych dla siedziby organu wnioskującego o udostępnienie danych przekazują corocznie Ministrowi Sprawiedliwości informację na temat przetwarzania danych telekomunikacyjnych, pocztowych i internetowych, z podziałem na liczbę przypadków udostępnienia danych dla danego rodzaju danych, oraz wyników przeprowadzonych kontroli, w terminie do dnia 31 marca roku następującego po roku nią objętym.
- § 2. Minister Sprawiedliwości przedstawia corocznie Sejmowi i Senatowi zagregowaną informację na temat przetwarzania danych telekomunikacyjnych, pocztowych i internetowych oraz wyników przeprowadzonych kontroli, w terminie do dnia 30 czerwca roku następującego po roku nią objętym.”.

- „6. Dane telekomunikacyjne lub internetowe, które nie mają znaczenia dla postępowania karnego lub postępowania karnego skarbowego, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu.
- 7. Szef Służby Celnej i dyrektor izby celnej prowadzą rejestry wystąpień o uzyskanie danych telekomunikacyjnych i internetowych zawierające informacje identyfikujące jednostkę organizacyjną Służby Celnej i funkcjonariusza uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Rejestry prowadzi się w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych.”;

18 lutego 2016 Rzecznik Praw Obywatelskich złożył do Trybunału Konstytucyjnego wniosek w sprawie nowelizacji ustawy o Policji.

- Rzecznik wnosi o zbadanie zgodności przepisów regulujących:
  - **stosowanie kontroli operacyjnej oraz podsłuchów,**
  - **pobieranie danych telekomunikacyjnych, pocztowych i internetowych**
- z Konstytucją RP, Konwencją o ochronie praw człowieka i podstawowych wolności oraz z Kartą Praw Podstawowych Unii Europejskiej.
- Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. z 2016 r., poz. 147), która wprowadziła do porządku prawnego większość kwestionowanych przepisów, nie tylko nie realizuje wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. (K 23/11), ale w poważnym zakresie narusza konstytucyjne prawa i wolności człowieka oraz standardy wyznaczone w prawie międzynarodowym.
- W zakresie pozyskiwania danych internetowych nie było konieczności żadnych zmian – wyrok Trybunału ich nie dotyczył.
- **Stanowisko RPO**
- Rzecznik Praw Obywatelskich nie kwestionuje – co do zasady – możliwości, a nawet potrzeby stosowania różnych form inwigilacji. Wymóg ochrony bezpieczeństwa nie ma jednak charakteru bezwzględnego i wyłącznego, co oznacza, że może podlegać ograniczeniom.
- Działania nakierowane na ochronę bezpieczeństwa obywateli nie mogą w sposób nieograniczony ingerować w prawo do prywatności. Zbyt duży zakres dopuszczalnej ingerencji oznacza ryzyko poważnych nadużyć Jest to szczególnie istotne w przypadku danych internetowych i tworzenia stałych łączy do ich pozyskiwania.
- Rzecznik Praw Obywatelskich podnosi w swoim wniosku liczne zarzuty, m.in.:
  - **brak granic czasowych lub nieproporcjonalnie długi czas trwania kontroli operacyjnej,**
  - **ograniczenie tajemnicy zawodowej,**
  - **nieograniczone pobieranie danych internetowych, telekomunikacyjnych, pocztowych,**
  - **brak realnej kontroli pobierania danych (jest tylko następcza kontrola sądowa),**
  - **brak następczego powiadamiania osoby, której dane były sprawdzane lub pobierane,**
  - **stosowanie przepisów uznanych przez Trybunał za niezgodne z Konstytucją RP.**

- **„Projekt ustawy wprowadzającej zmianę zasad niejawnego pozyskiwania informacji o osobach w dalszym ciągu nie wykonuje wyroku Trybunału Konstytucyjnego" – wynika z opinii Helsińskiej Fundacji Praw Człowieka do projektu ustawy zmieniającej ustawę o Policji.**
- Poselski projekt ustawy skierowany niedawno do Sejmu ma na celu wykonanie wyroku Trybunału Konstytucyjnego z lipca 2014 r. Projekt bazuje w przeważającej większości na rozwiązaniach zawartych w senackim projekcie z lipca 2015 r., który ostatecznie nie został uchwalony. HFPC wskazywała już wtedy, że projekt nie tworzy systemu niezależnej uprzedniej kontroli nad pozyskiwaniem danych telekomunikacyjnych (opinia z sierpnia 2015 r. dostępna jest tutaj). Tym samym, projekt nie realizuje wytycznych wynikających z prawa Unii Europejskiej dotyczących zasad ochrony danych osobowych.
- Niestety, także projekt poselski z grudnia 2015 r. nie tworzy systemu niezależnej kontroli nad działaniami służb. „Kontrola następcza prowadzona przez sąd okręgowy oparta o analizę sprawozdań przedstawianych co pół roku przez służby nie zabezpieczy przed możliwością nadużyć" – wskazuje Barbara Grabowska-Moroz, prawniczka HFPC.
- Co więcej, kompetencja udostępniania służbom danych została poszerzona o tzw. dane internetowe, do których dostęp będzie możliwy bez każdorazowych wniosków, ale za pomocą sieci teleinformatycznej.
- „Zakres danych internetowych jest tak szeroki, że istnieje realne ryzyko, że będą ona obejmowały m.in. adresy przeglądanych stron internetowych czy nawet treść komunikacji" – ocenia Barbara Grabowska-Moroz.
- Projekt poselski, podobnie jak projekt z lipca 2015 r., nie gwarantuje odpowiedniej ochrony tajemnic zawodowych, np. adwokackiej czy dziennikarskiej. Projekt nakazuje przekazanie takich informacji prokuratorowi, który nie będzie uprawniony do zarządzenia ich zniszczenia, a następnie informacje te zostaną przekazane sądowi.
- „Tym samym obowiązek niezwłocznego komisyjnego zniszczenia tych danych, wynikający z wyroku TK, przybiera formę procedury umożliwiającej „legalizację" zgromadzonych informacji zawierających treści objęte tajemnicą zawodową" – ocenia Barbara Grabowska-Moroz.
- Projekt poszerza również zakres tzw. kontroli operacyjnej przewidując, że będzie ona obejmować, m.in. uzyskiwanie i utrwalanie „danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych". W ocenie Helsińskiej Fundacji Praw Człowieka, takie rozwiązanie pogarsza sytuację jednostki. Obecnie dokonanie takich czynności wymaga postanowienia prokuratora, zaś osoba, której prawa zostały w ten sposób naruszone może złożyć zażalenie. W świetle projektowanych przepisów osoba, której komputer został w ten sposób przeszukany, najprawdopodobniej może się o tym nigdy nie dowiedzieć. Wynika to z kolei faktu, że projekt w dalszym ciągu nie wykonuje postanowienia sygnalizacyjnego Trybunału Konstytucyjnego, który nakazał wprowadzenie obowiązku poinformowania osoby poddanej kontroli operacyjnej o fakcie jej prowadzenia i zakończenia.

Dz.U. 2002 Nr 144 poz. 1204

USTAWA z dnia 18 lipca 2002 r.

o świadczeniu usług drogą elektroniczną

- **Art. 18.** 1. Usługodawca może przetwarzać następujące dane osobowe usługobiorcy niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego między nimi:
  - 1) nazwisko i imiona usługobiorcy;
  - 2) numer ewidencyjny PESEL lub – gdy ten numer nie został nadany – numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość;
  - 3) adres zameldowania na pobyt stały;
  - 4) adres do korespondencji, jeżeli jest inny niż adres, o którym mowa w pkt 3;
  - 5) dane służące do weryfikacji podpisu elektronicznego usługobiorcy;
  - 6) adresy elektroniczne usługobiorcy.

Dz.U. 2002 Nr 144 poz. 1204

- 2. W celu realizacji umów lub dokonania innej czynności prawnej z usługobiorcą, usługodawca może przetwarzać inne dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia.
- 3. Usługodawca wyróżnia i oznacza te spośród danych, o których mowa w ust. 2, jako dane, których podanie jest niezbędne do świadczenia usługi drogą elektroniczną zgodnie z art. 22 ust. 1.
- 4. Usługodawca może przetwarzać, za zgodą usługobiorcy i dla celów określonych w art. 19 ust. 2 pkt 2, inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną.
- 5. Usługodawca może przetwarzać następujące dane charakteryzujące sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną (**dane eksploatacyjne**):
  - 1) oznaczenia identyfikujące usługobiorcę nadawane na podstawie danych, o których mowa w ust. 1;
  - 2) oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca;
  - 3) informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną;
  - 4) informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną.
- 6. Usługodawca udziela informacji o danych, o których mowa w ust. 1–5, organom państwa na potrzeby prowadzonych przez nie postępowań.

Dz.U. 2002 Nr 144 poz. 1204

- Art. 19. 1. Usługodawca nie może przetwarzać danych osobowych usługobiorcy po zakończeniu korzystania z usługi świadczonej drogą elektroniczną, z zastrzeżeniem ust. 2.
- 2. Po zakończeniu korzystania z usługi świadczonej drogą elektroniczną usługodawca, na zasadach określonych w ust. 3-5, może przetwarzać tylko te spośród danych określonych w art. 18, które są:
  - 1) niezbędne do rozliczenia usługi oraz dochodzenia roszczeń z tytułu płatności za korzystanie z usługi;
  - 2) niezbędne do celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców z przeznaczeniem wyników tych badań na potrzeby polepszenia jakości usług świadczonych przez usługodawcę, za zgodą usługobiorcy;
  - 3) niezbędne do wyjaśnienia okoliczności niedozwolonego korzystania z usługi, o którym mowa w art. 21 ust. 1;
  - 4) dopuszczone do przetwarzania na podstawie odrębnych ustaw lub umowy.
- 3. Rozliczenie usługi świadczonej drogą elektroniczną przedstawione usługobiorcy nie może ujawniać rodzaju, czasu trwania, częstotliwości i innych parametrów technicznych poszczególnych usług, z których skorzystał usługobiorca, chyba że zażądał on szczegółowych informacji w tym zakresie.
- 4. Dla celów, o których mowa w ust. 2 pkt 2, dopuszcza się jedynie zestawianie danych wymienionych w art. 18 ust. 4 i 5 dotyczących korzystania przez usługobiorcę z różnych usług świadczonych drogą elektroniczną, pod warunkiem usunięcia wszelkich oznaczeń identyfikujących usługobiorcę lub zakończenie sieci telekomunikacyjnej albo system teleinformatyczny, z którego korzystał (anonimizacja danych), chyba że usługobiorca wyraził uprzednio zgodę na nieusuwanie tych oznaczeń.
- 5. Usługodawca nie może zestawiać danych osobowych usługobiorcy z przybranym przez niego pseudonimem.

dane internetowe

- Nie tylko w stosunku do **billingów** (czyli zestawów połączeń, rozmów, SMS-ów wysyłanych przez abonentów), ale także owych **"danych internetowych"**. A te zgodnie z UŚUDE, do której odwołuje się projekt, stanowią pokaźny katalog: od powiązania imienia i nazwiska internauty z jego IP (indywidualny numer danego połączenia sieciowego) przez internetową korespondencję, na wykazie sieciowego ruchu (kiedy, na jakie strony i na jaki czas wchodzono) kończąc. To baza wiedzy większa niż dane telekomunikacyjne. *Problemem jest i to, że w przeciwieństwie do danych telekomunikacyjnych dostawcy **usług internetowych** nie mają obowiązku przechowywania danych użytkowników. Nowy obowiązek nie został połączony z wyjaśnieniem, jak powinni je przetwarzać*.
- inaczej jest w przypadku działalności telekomunikacyjnej. Art. 180a PT wyraźnie nakłada na operatorów obowiązek retencji danych telekomunikacyjnych przez 12 miesięcy — a służby mają uprawnienie do myszkowania w tych danych na podst. art. 180d PT — ale w odniesieniu do serwisów świadczących usługi elektroniczne przepisu takiego nie ma.

Dz.U. 2004 Nr 171 poz. 1800
USTAWA z dnia 16 lipca 2004 r.
Prawo telekomunikacyjne

Art. 161. 1. Z zastrzeżeniem ust. 2, treści lub dane objęte tajemnicą telekomunikacyjną mogą być zbierane, utrwalane, przechowywane, opracowywane, zmieniane, usuwane lub udostępniane tylko wówczas, gdy czynności te, zwane dalej „przetwarzaniem”, dotyczą usługi świadczonej użytkownikowi albo są niezbędne do jej wykonania. Przetwarzanie w innych celach jest dopuszczalne jedynie na podstawie przepisów ustawowych.

- 2. Dostawca publicznie dostępnych usług telekomunikacyjnych jest uprawniony do przetwarzania następujących danych dotyczących użytkownika będącego osobą fizyczną:
  - 1) nazwisk i imion;
  - 2) imion rodziców;
  - 3) miejsca i daty urodzenia;

- 4) adresu miejsca zamieszkania i adresu korespondencyjnego jeżeli jest on inny niż adres miejsca zamieszkania;
- 5) numeru ewidencyjnego PESEL – w przypadku obywatela Rzeczypospolitej Polskiej;
- 6) nazwy, serii i numeru dokumentów potwierdzających tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej – numeru paszportu lub karty pobytu;
- 7) zawartych w dokumentach potwierdzających możliwość wykonania zobowiązania wobec dostawcy publicznie dostępnych usług telekomunikacyjnych wynikającego z umowy o świadczenie usług telekomunikacyjnych.

- 3. Oprócz danych, o których mowa w ust. 2, dostawca publicznie dostępnych usług telekomunikacyjnych może, za zgodą użytkownika będącego osobą fizyczną, przetwarzać inne dane tego użytkownika w związku ze świadczoną usługą, w szczególności numer konta bankowego lub karty płatniczej, a także adres poczty elektronicznej oraz numery telefonów kontaktowych.

Art. 180. 1. Przedsiębiorca telekomunikacyjny jest obowiązany do niezwłocznego blokowania połączeń telekomunikacyjnych lub przekazów informacji, na żądanie uprawnionych podmiotów, jeżeli połączenia te mogą zagrażać obronności, bezpieczeństwu państwa oraz bezpieczeństwu i porządkowi publicznemu, albo do umożliwienia dokonania takiej blokady przez te podmioty.

2. Operator ruchomej publicznej sieci telekomunikacyjnej jest obowiązany do:

- 1) uniemożliwienia używania w jego sieci skradzionych telekomunikacyjnych urządzeń końcowych;
- 2) przekazywania informacji identyfikujących skradzione telekomunikacyjne urządzenia końcowe innym operatorom ruchomych publicznych sieci telekomunikacyjnych w celu realizacji przez nich czynności, o których mowa w pkt 1.

- 3. Czynności, o których mowa w ust. 2, dokonywane są przez operatora w terminie 1 dnia roboczego od dnia przedstawienia przez abonenta poświadczenia zgłoszenia kradzieży telekomunikacyjnego urządzenia końcowego, numeru identyfikacyjnego tego urządzenia i dowodu jego nabycia lub innych danych jednoznacznie identyfikujących właściciela tego urządzenia. W przypadku uzyskania informacji identyfikujących skradzione urządzenia od innego operatora, termin 1 dnia roboczego liczy się od tej daty.

Art. 180a. 1. Z zastrzeżeniem art. 180c ust. 2 pkt 2, operator publicznej sieci telekomunikacyjnej oraz dostawca publicznie dostępnych usług telekomunikacyjnych są obowiązani na własny koszt:

- 1) zatrzymywać i przechowywać dane, o których mowa w art. 180c, generowane w sieci telekomunikacyjnej lub przez nich przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi;
- 2) udostępniać dane, o których mowa w pkt 1, uprawnionym podmiotom, a także Służbie Celnej, sądowi i prokuratorowi, na zasadach i w trybie określonych w przepisach odrębnych;
- 3) chronić dane, o których mowa w pkt 1, przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem, zgodnie z przepisami art. 159–175a, art. 175c i art. 180e.

- 2. Z zastrzeżeniem ust. 3, obowiązek, o którym mowa w ust. 1, uważa się za wykonany, jeżeli operator publicznej sieci telekomunikacyjnej lub dostawca publicznie dostępnych usług telekomunikacyjnych w przypadku zaprzestania działalności telekomunikacyjnej, przekaże dane do dalszego przechowywania, udostępniania oraz ochrony innemu operatorowi publicznej sieci telekomunikacyjnej lub dostawcy publicznie dostępnych usług telekomunikacyjnych.

- **Art. 180c.** 1. Obowiązkiem, o którym mowa w art. 180a ust. 1, objęte są dane niezbędne do:
  - 1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego:
    - a) inicjującego połączenie,
    - b) do którego kierowane jest połączenie;
  - 2) określenia:
    - a) daty i godziny połączenia oraz czasu jego trwania,
    - b) rodzaju połączenia,
    - c) lokalizacji telekomunikacyjnego urządzenia końcowego.

- **Art. 180e.** W celu ochrony danych, o której mowa w art. 180a ust. 1 pkt 3, przedsiębiorca telekomunikacyjny stosuje właściwe środki techniczne i organizacyjne oraz zapewnia dostęp do tych danych jedynie upoważnionym pracownikom.

dane internetowe

- Ustawa wspomina o tzw. danych internetowych do których służby będą miały teraz prosty i niekontrolowany dostęp.
- Co to są dane internetowe? Dane internetowe to dane, zbierane automatycznie przez dostawców Internetu. Na dane te składają się następujące informacje:
  - kiedy i jak długo korzystamy z Internetu
  - na jakie strony wchodzimy
  - jakie hasła wpisujemy w przeglądarkę i jakich informacji szukamy
- Dzięki temu Policja czy prokuratura może wiedzieć, że wchodzisz na strony porno, jak długo na nich zostajesz i czy faktycznie coś oglądasz (jak dużo MB ściągasz). Jedyne czego wiedzieć nie będą to czy oglądasz gołych Panów czy tzw. MILF'y.
- Teoretycznie policja nie może sprawdzać Internautów na wyrywki. Jednak prawda jest taka, ze wcale nie musimy być przestępcami by znaleźć się na celowniku. W końcu policja ma też zapobiegać przestępstwom i pod takie działanie można podciągnąć różnego typu działania (szczególnie gdy odbywają się poza kontrolą sądu!).

są dane internetowe

- Czym są dane internetowe, podaje ustawa o świadczeniu usług drogą elektroniczną.
- W uproszczeniu dzielą się na dane
- Stałe (- to inaczej dane osobowe - imię, nazwisko, adres, numer PESEL, numer IP etc.)
- Eksploatacyjne (- to te, które internauta tworzy, surfując po sieci. To one mają kluczowe znaczenie, bo tworzą nasz życiorys w sieci, są opisem całej naszej aktywności internetowej).

[Służby] będą miały dostęp do tzw. metadanych - gdzie, o której godzinie i jak długo byłeś. Nic nie da wyczyszczenie ciasteczek (cookies) w przeglądarce czy skorzystanie w niej z trybu incognito. Twój dostawca internetu i tak rejestruje odwiedzane przez ciebie strony, a więc zobaczą to też służby. Do tej pory służby mogły o to prosić, a firma mogła odmówić.

Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny

Investigatory Powers Bill

- Since publication in December last year, the government's Draft Investigatory Powers Bill has sparked debate over the balance between privacy concerns and national security in the post-Snowden era, with controversy around encryption, bulk data and hacking, to name just a few aspects.
- ***Updated 15th February 2016:*** The draft investigatory powers bill has now been criticised by three joint committees: the science and technology committee on February 1, the intelligence and security committee on February 9 and most importantly, the joint committee for the bill itself on February 11.

- The joint committee for the draft investigatory powers bill made 86 recommendations for changes to the bill in its report, concentrating on issues of clarity, judicial oversight and justification of the various powers. For a summary of these suggestions skip ahead one section.
- **The headlines**
- Clause 71 has led the news agenda so far. This requires web and phone companies (CSPs) to store records of websites visited by every citizen for 12 months for access by police, security services and other public bodies.
- In practice this would take the form of an itemised list of each citizen's browsing history. This would not be a list of the specific web pages but the main domain (so computerworlduk.com but not the specific stories you read) so a basic online footprint can be drawn up. One concern here will be around the security of this data, especially in the current climate of TalkTalk customer hacks and data dumps.
- The bill seeks to make the power for security services to acquire bulk collections of communications data explicitly legal. For example this could mean a bulk data set such as NHS health records.
- Security services will also be legally empowered to bug computers and phones upon approval of a warrant. Companies will be legally obliged to assist these operations and bypass encryption where possible (more on this below).

Projet de loi relatif au renseignement

- La loi a été promulguée le 24 juillet 2015. Elle a été publiée au Journal officiel de la République française dans lequel sont publiés les lois et les règlements. du 26 juillet 2015.

6:59AM GMT 01 Mar 2016

- SIR – Intelligence agencies and the police require strong surveillance powers. Their powers and responsibilities – as well as their limits – must be clear to be effective.
- All three parliamentary reports on the draft Investigatory Powers Bill concluded that it does not meet the requirements of clarity, consistency and coherence. They call for new drafting, further safeguards, further evidence and further consultation.
- Given these recommendations, the Government's intention to pass the Investigatory Powers Bill this year is not in the nation's interest. There is no need to be bound by this time frame. The powers, which expire this year, to give law enforcement access to data could be dealt with as a separate Bill. This would allow a comprehensive Investigatory Powers Act to follow next year after adequate consultation.
- Surveillance is a global concern, and this new law, if done right, could lead the world. It will affect security, freedom and commerce. We must give the Bill the time it needs – not rush it through Parliament. We urge the Government to think again.

INTERCEPTION

What is it?

18. Interception is the obtaining of the content of a communication – such as a telephone call, email or social media message – in the course of its transmission or while stored on a telecommunications system. Interception is used to collect valuable intelligence against terrorists and serious criminals, which can inform law enforcement and national security investigations as well as support military operations.

Why do we need it?

19. Warranted interception is used only for intelligence purposes. It is a vital tool which helps the law enforcement and security and intelligence agencies to prevent and detect serious or organised crime, and to protect national security.

What happens now?

20. Warranted interception is governed by RIPA. It allows for the security and intelligence agencies, the armed forces and a small number of law enforcement agencies to seek warrants when it is necessary and proportionate to do so for one of three statutory purposes: in the interests of national security; for the prevention and detection of serious crime; or in the interests of the economic well-being of the UK where it is connected to national security. Separate provision for interception of wireless telegraphy (such as military radio communications) is made under the Wireless Telegraphy Act 2006.

COMMUNICATIONS DATA

What is it?

25. Communications data is information about communications: the 'who', 'where', 'when', 'how' and 'with whom' of a communication but not what was written or said. It includes information such as the subscriber to a telephone service. Law enforcement, the security and intelligence agencies and other specified public authorities may acquire this data from Communications Service Providers (CSPs) who may be required to retain it.

Why do we need it?

26. Communications data is an essential tool for the full range of law enforcement activity and national security investigations. Requests may be made for data in order to identify the location of a missing person or to establish a link (through call records) between a suspect and a victim. It is used to investigate crime, keep children safe, support or disprove alibis and tie a suspect to a particular crime scene, among many other things.

Sometimes communications data is the only way to identify offenders, particularly where offences are committed online, such as child sexual exploitation or fraud.

EQUIPMENT INTERFERENCE

What is it?

32. Equipment interference allows the security and intelligence agencies, law enforcement and the armed forces to interfere with electronic equipment such as computers and smartphones in order to obtain data, such as communications, from a device.

Equipment interference encompasses a wide range of activity, from remote access to computers to downloading covertly the contents of a mobile phone during a search.

Why do we need it?

33. Where necessary and proportionate the security and intelligence agencies, law enforcement and the armed forces need to be able to access communications or other information held on computers, in order to gain valuable intelligence in national security and serious crime investigations and to help gather evidence for use in criminal prosecutions.

Equipment interference plays an important role in mitigating the loss of intelligence that may no longer be obtained through other techniques, such as interception, as a result of sophisticated encryption. It can sometimes be the only method by which to acquire the data. The armed forces use this technique in some situations to gather data in support of military operations.

BULK POWERS

What are they?

38. Access to bulk data is crucial in enabling the security and intelligence agencies to investigate known, high-priority threats and to identify emerging threats from individuals not previously known to them. The law provides for the use of interception, communications data and equipment interference powers in bulk. These can be used to obtain large volumes of data that are likely to include communications or other data relating to terrorists and serious criminals. Robust safeguards govern access to this data to ensure it is only examined where it is necessary and proportionate to do so.

BULK POWERS

Why do we need them?

39. The security and intelligence agencies frequently have only small fragments of intelligence or early unformed leads about people overseas who pose a threat to the UK. Equally, terrorists, criminals and hostile foreign intelligence services are increasingly sophisticated at evading detection by traditional means. Access to bulk data enables the security and intelligence agencies to:

- Obtain intelligence on overseas subjects of interest, including threats to UK citizens and our armed forces;Identify threats here in the UK, sometimes from fragments of intelligence;
- Establish and investigate links between known subjects of interest, at pace, in complex investigations;Understand known suspects' behaviour and communications methods to identify potential attack planning;
- Verify information obtained about subjects of interest through other sources (e.g. agents); and
- Resolve sometimes anonymous online personae to real world identities

40. Bulk powers are used to advance investigations both in the UK and overseas. They are integral to the work of the security and intelligence agencies.

INTERNET CONNECTION RECORDS

What are they?

49. An internet connection record (ICR) is a record, comprised of a number of items of communications data, of an event about the service to which a customer has connected to on the internet, such as a website or instant messaging application. It is captured by the company providing access to the internet. Where available, this data may be acquired from CSPs by law enforcement and the security and intelligence agencies.

50. An ICR is not a person's full internet browsing history. It is a record of the services that they have connected to, which can provide vital investigative leads. It would not reveal every web page that they visit or anything that they do on that web page.

INTERNET CONNECTION RECORDS

Why do we need them?

51. ICRs are vital to law enforcement investigations in a number of ways. For example:

- To assist in identifying who has sent a known communication online, which often involves a process referred to as internet protocol (IP) address resolution
- To establish what services a known suspect or victim has used to communicate online, allowing investigators to request more specific communications data
- To establish whether a known suspect has been involved in online criminality, for example sharing indecent images of children, accessing terrorist material or fraud
- To identify services a suspect has accessed which could help in an investigation including, for example, mapping services.

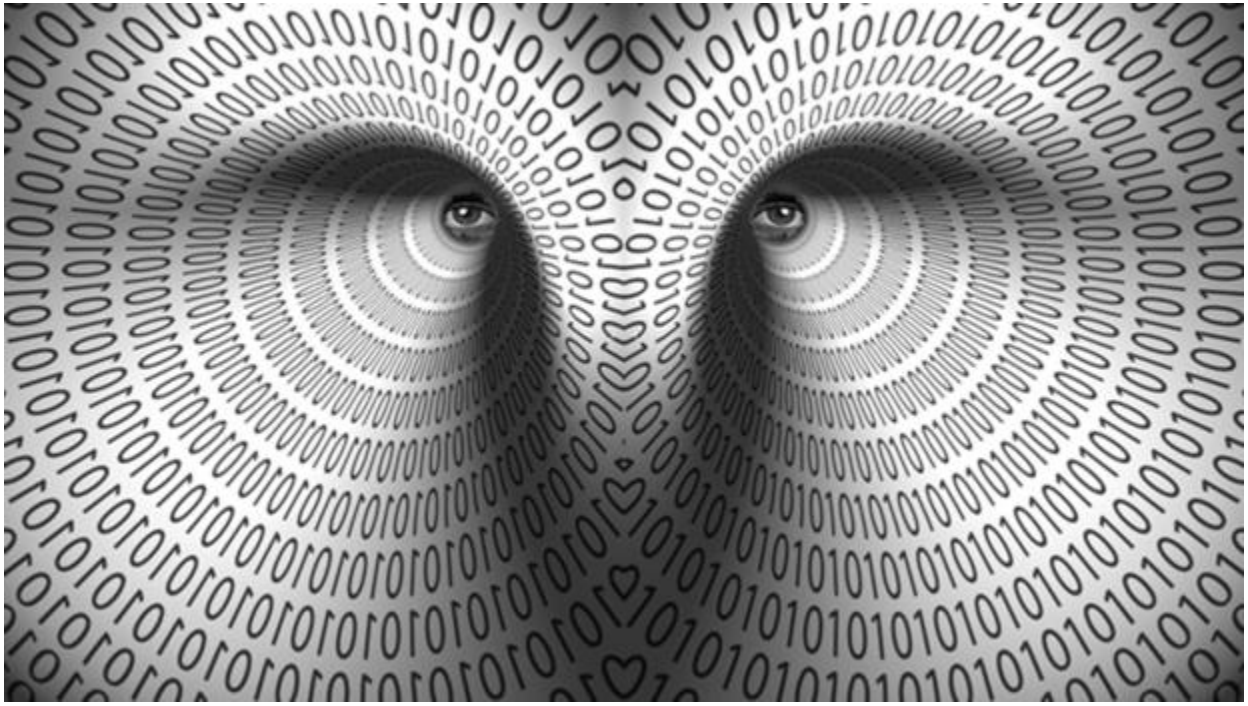
BULK PERSONAL DATASETS

What are they?

74. Bulk Personal Datasets (BPDs) are sets of personal information about a large number of individuals, the majority of whom will not be of any interest to the security and intelligence agencies. The datasets are held on electronic systems for the purpose of analysis by the security and intelligence agencies. Examples of these datasets include the electoral roll, telephone directories and travel-related data.

Why do we need them?

75. BPDs are essential in helping the security and intelligence agencies identify subjects of interest or individuals who surface during the course of an investigation, to establish links between individuals and groups, to understand better a subject of interest's behaviour and connections and quickly to exclude the innocent. In short, they enable the agencies to join the dots in an investigation and to focus their attention on individuals or organisations that threaten our national security.




SURVEILLANCE


Terror attacks in Paris

PARIS, 13 NOVEMBRE 2015

On the run

Salah Abdeslam **(Wanted)**

Mohamed Abrini **(Wanted)**

Stade de France

Bilal Hadfi (Dead)

'Ahmad al-Mohammed' (Dead)

'M al Mahmod' (Dead)

Bars and restaurants

Unnamed attacker (Dead)

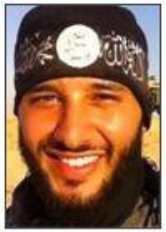
Abdelhamid Abaaoud (Dead) Suspected ringleader

Brahim Abdeslam (Dead)

Bataclan

Omar Ismail Mostefai (Dead)

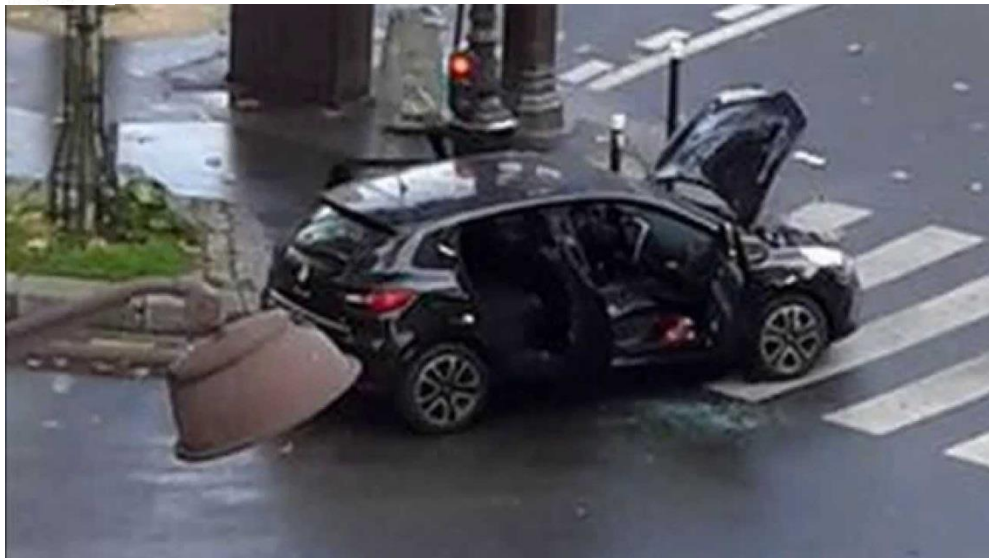
Samy Amimour (Dead)



Foued Mohamed-Aggad (Dead)

Source: Pictures AFP, EVN, EPA, Belgian Police

BBC



First on CNN: Paris attackers likely used encrypted apps, officials say


By Evan Perez and Shimon Prokupecz, CNN

Updated 1500 GMT (2300 HKT) December 17, 2015

BOINGBOING / CORY DOCTOROW / 5:58 PM TUE

If the Paris attackers weren't using crypto, the next ones will, and so should you

Lots of law enforcement agencies hate crypto, because the technology that helps us protect our communications from criminals and griefers and stalkers and spies also helps criminals keep secrets from cops. With each terrorist attack there's a fresh round of doom-talk from spooks an cops about the criminals "going dark" -- as though the present situation in which the names and personal information of everyone who talks to everyone else, all the time, where they are then they talk, where they g and who they talk to next, is somehow *less* surveillant than the past, whe cops could sometimes use analog tape-recorders to wiretap the very fe

Londyn 7 lipca 2005

If the FBI wins, it could open the door to massive surveillance

The first thing to understand about Apple's latest fight with the FBI—over a court order to help unlock the deceased San Bernardino shooter's phone—is that it has very little to do with the San Bernardino shooter's phone.

It's not even, really, the latest round of the Crypto Wars—the long running debate about how law enforcement and intelligence agencies can adapt to the growing ubiquity of uncrackable encryption tools.

Rather, it's a fight over the future of high-tech surveillance, the trust infrastructure undergirding the global software ecosystem, and how far technology companies and software developers can be conscripted as unwilling suppliers of hacking tools for governments. It's also the public face of a conflict that will undoubtedly be continued in secret—and is likely already well underway.

First, the specifics of the case. The FBI wants Apple's help unlocking the work iPhone used by Syed Farook, who authorities believe perpetrated last year's mass killing at an office Christmas party before perishing in a shootout with police. They've already obtained plenty of information about Farook's activities from Apple's iCloud servers, where much of his data was backed up, and from other communications providers such as Facebook. It's unclear whether they've been able to recover any data from two other mobile devices Farook physically destroyed before the attack, which seem most likely to have contained relevant information. Julian Sanchez TIME Feb. 18, 2016


The Unlocked iPhone 5c Clarified that no other Conspirators were involved in San Bernardino's Terrorist Attack
Patently Apple

ALE ……

- **Hakerzy działający na zlecenie brytyjskiego tabloidu "News of the World" włamywali się do poczty głosowej krewnych żołnierzy poległych w Afganistanie i Iraku oraz ofiar zamachów terrorystycznych - twierdzi dziennik "Daily Telegraph". Gazeta pisze, iż w mieszkaniu Glena Mulcaire'a, prywatnego detektywa wynajętego przez "NotW" dla zakładania podsłuchów, policja znalazła numery telefonów komórkowych członków rodzin poległych żołnierzy i ofiar zamachu terrorystycznego w Londynie z 7 lipca 2005 roku.**

Liczba aresztowanych w brytyjskiej aferze podsłuchowej przekroczyła 100

bart | 18.01.2013 , aktualizacja: 17.01.2013 23:34

Rupert Murdoch (Fot. HO Reuters)

Dziennikarz śledczy tabloidu "The Sun" i dwóch policjantów to kolejne osoby, które zostały zatrzymane w związku z trwającą od prawie dwóch lat aferą wokół medialnego koncernu Ruperta Murdocha. Jego dziennikarze włamywali się do poczt głosowych znanych ludzi i korumpowali funkcjonariuszy.

Niespełna 40-letni Anthony France był w redakcji "The Sun" gwiazdą. By udowodnić, że brytyjski parlament jest fatalnie pilnowany, przemycił do jego gmachu atrapę bomby. Potem dzięki fałszywym referencjom zatrudnił się w nim jako kelner, dzięki czemu miał dostęp do najważniejszych polityków w państwie.

W czwartek rano do jego mieszkania na północnych przedmieściach Londynu wkroczyli policjanci, którzy zabrali dziennikarza na posterunek. Śledczy prowadzący operację o kryptonimie "Elveden" zarzucają mu, że w zamian za informacje płacił funkcjonariuszom łapówki.

DUBLIN, December 21, 2011

- The Irish Data Protection Commission today concluded that Facebook has “a positive approach and commitment” to protecting the privacy of its international users, though it did get Facebook to agree to provide further notifications and improve its policies in a few areas.
- You might be surprised that what Ireland has to say about regulating Facebook privacy is terribly important — but it actually is. **Because Facebook’s international headquarters are in Dublin**, this local commission oversees Facebook’s compliance in all regions other than the U.S. and Canada.

Facebook agreed to make changes in time for a follow-up Irish Data Protection Commission audit in July 2012.

- Creating additional notifications explaining photo tagging using facial recognition (which has been a particularly contentious feature in Europe)
- Reducing data retention and logging for people who are not logged into Facebook (so-called “logged-out cookies” and alleged “shadow profiles” of non-members have been another reason for recent outcry)
- Telling users more about how to control when their information is given to Facebook platform applications

FTC

- As compared to Facebook's recent settlement with the American Federal Trade Commission, the Irish audit seems to be about more up-to-date privacy issues (much of the FTC stuff dated back to 2009). The FTC settlement is also a longer-term arrangement, with Facebook agreeing to 20 years of privacy audits. And Mark Zuckerberg didn't give Ireland a formal apology, admitting to making "a bunch of mistakes."

Teacher Stern LLP 37-41 Bedford Row London WC1R 4JH

- Advice for Facebook users remains to be cautious about putting too much personal information on your profile and to review your privacy settings regularly to ensure that you are protected from third party websites receiving information. Given the recent interest shown in Facebook by the Information Commissioner°Øs Office there may well be further developments.

Brussels, 25 January 2012 – **The European Commission** has today proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. Technological progress and globalisation have profoundly changed the way our data is collected, accessed and used. In addition, the 27 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement. A single law will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The initiative will help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe.

- W dniu 25 stycznia 2012 r. Komisja przyjęła pakiet zmian regulacji UE w zakresie ochrony danych, w tym wniosek dotyczący rozporządzenia zawierającego ogólne regulacje w zakresie ochrony danych oraz wniosek dotyczący dyrektywy zawierającej szczególne regulacje dotyczące ochrony danych dla sektora odpowiedzialnego za egzekwowanie prawa.

KOMISJA EUROPEJSKA

Bruksela, dnia 25.1.2012 r.
COM(2012) 10 final

2012/0010 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych

[…]

KOMISJA EUROPEJSKA

Bruksela, dnia 25.1.2012 r.
COM(2012) 11 final

2012/0011 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)

(Tekst mający znaczenie dla EOG)

{SEC(2012) 72 final}
{SEC(2012) 73 final}

Unijną dyrektywę o ochronie danych osobowych zastąpi rozporządzenie. Zasady ochrony danych osobowych w sektorze policji i wymiaru sprawiedliwości określi dyrektywa.
Rozporządzenie to akt, który obowiązuje bezpośrednio w krajach członkowskich, bez potrzeby wydawania aktów prawnych wdrażających je do porządku krajowego. Dzięki jego wprowadzeniu nastąpi pełna harmonizacja prawa materialnego w ramach UE.
Komisarz Viviane Reding poinformowała też, że zasady ochrony danych osobowych w policji i wymiarze sprawiedliwości w sprawach karnych uregulowane zostaną w dyrektywie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy w celu zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania sankcji karnych i swobodnego przepływu tych danych. Jej projekt również oficjalnie zaprezentowano 25 stycznia 2012 r.

W opinii dra Wojciecha Rafała Wiewiórowskiego, Generalnego Inspektora Ochrony Danych Osobowych (GIODO), proponowane zmiany idą w dobrym kierunku. Dzięki ich wprowadzeniu powstanie wspólny rynku przepływu informacji, a jednocześnie zapewniona zostanie odpowiednia ochrona danych osobowych przed działaniami z zewnątrz UE i przy przekazywaniu danych do państw trzecich. Projektowane przepisy są odświeżone pod względem terminologii, która jest używana w świecie nowych technologii. Jednocześnie są one technologicznie neutralne, tzn. nie opisują konkretnych modeli biznesowych czy technologii, lecz wprowadzają rozwiązania prawne umożliwiające rozwiązanie problemów występujących w związku z wykorzystywaniem nowoczesnych technologii.

Po ponad czterech latach prac, w kwietniu 2016 roku, PE i Rada przyjęły nowe przepisy w tej materii – pkt. 1 i 2 (pakiet legislacyjny został przyjęty w dwóch czytaniach).

Nowe przepisy zawarte w rozporządzeniu:
- powiększają katalog praw przysługujących osobom, których dane są przetwarzane;
- regulują m.in.: prawo do usunięcia lub sprostowania danych oraz "prawo do bycia zapomnianym";
- regulują warunki wyrażenia zgody na przetwarzanie danych prywatnych oraz kwestie zgłaszania naruszenia ochrony danych osobowych i prawo osoby, której dane dotyczą, do informacji o naruszeniu ochrony danych;
- zapewniają prawo do przenoszenia danych do innego usługodawcy;
- zapewniają prowadzenie polityki prywatności w sposób przejrzysty i zrozumiały dla użytkownika;
- przewidują kary pieniężne dla administratorów i podmiotów przetwarzających za naruszanie przepisów (nawet w wysokości 4% całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego).
Rozporządzenie przewiduje również ustanowienie Europejskiej Rady Ochrony Danych, która skupiałaby przedstawicieli wszystkich 28 niezależnych organów nadzorczych.

Dyrektywa z kolei określa m.in. minimalne normy dotyczące przetwarzania danych osobowych dla potrzeb policji i sądów oraz swobodnego przepływu tych danych we wszystkich państwach UE.

Ponadto, nowe przepisy zawarte w rozporządzeniu i dyrektywie określają obowiązki administratora danych, regulują kwestie przekazywania danych do państwa trzeciego oraz przyznają osobom, których dane są przetwarzane, prawo do odszkodowania za ewentualne szkody wynikające z ich nieprzepisowego przetwarzania.

Rozporządzenie weszło w życie 24 maja 2016, będzie stosowane bezpośrednio w państwach członkowskich od 25 maja 2018. Również 2 lata przysługują państwom członkowskim na wdrożenie przepisów dyrektywy (w Wielkiej Brytanii i Irlandii dyrektywa będzie miała zastosowanie jedynie w ograniczonym stopniu; Dania ma 6 miesięcy - od daty przyjęcia dyrektywy – na podjęcie decyzji o jej ewentualnej transpozycji do krajowego prawodawstwa).

Aktualności

- Szkolenie dla przedstawicieli Poczty Polskiej S.A.
- Oświadczenie prasowe Grupy Roboczej art. 29
- Cykl szkoleń GIODO dla radców prawnych
- Wyniki ankiety Eurobarometru o wpływie cyberprzestępczości
- Obradowała Rada Naukowa GIODO, 20.11.2013 r.
- GIODO gościem XVII Kongresu ABI, 13-14.11.2013 r.

Ważne

- VIII Dzień Ochrony Danych, 28 stycznia 2014 r.
- GIODO nie grozi

Informacje Ogólne

INFORMACJE OGÓLNE

Metadane

W dniu 25 stycznia 2012 r. Komisja przyjęła pakiet zmian regulacji UE w zakresie ochrony danych, w tym wniosek dotyczący **rozporządzenia** zawierającego ogólne regulacje w zakresie ochrony danych oraz wniosek dotyczący **dyrektywy** zawierającej szczególne regulacje dotyczące ochrony danych dla sektora odpowiedzialnego za egzekwowanie prawa

Planowane jest zastąpienie dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych rozporządzeniemParlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Rozporządzenie to akt, który obowiązywałby bezpośrednio w krajach członkowskich, bez potrzeby wydawania aktów prawnych wdrażających je do porządku krajowego. Dzięki jego wprowadzeniu nastąpiłaby pełna harmonizacja prawa materialnego w ramach UE i swobodnego przepływu tych danych.

Natomiast nowością w polskim systemie prawnym będzie dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy w celu zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania sankcji karnych i swobodnego przepływu tych danych, jako że zasady zawarte w zaprezentowanym projekcie nie są obecne w istniejących dziś polskich przepisach prawa.

DOKUMENTY

[346 kB] Sprawozdanie Komisji dla Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów — Metadane

- Reforma unijnych przepisów
  - Europejski Inspektor Ochrony Danych
  - Grupa Robocza Artykułu 29 ds. Ochrony Danych
  - Informacje Ogólne
  - Komisja Europejska
  - Konsultacje GIODO
  - Parlament Europejski
  - Rada
- Przepisy prawa
- Wyroki
- Decyzje GIODO
- Wystąpienia, sygnalizacje, wnioski GIODO

JEŚLI CHCESZ ZŁOŻYĆ SKARGĘ

What will be the key changes?

- A **‘right to be forgotten’** will help people better manage data-protection risks online. When they no longer want their data to be processed and there are no legitimate grounds for retaining it, the data will be deleted.
- **Whenever consent is required** for data processing, it will have to be given **explicitly**, rather than be assumed.
- Easier access to one’s own data and the **right of data portability**, i.e. easier **transfer of personal data** from one service provider to another.
- Companies and organisations will have to notify serious data breaches without undue delay, **where feasible within 24 hours**.
- **A single set of rules** on data protection, valid across the EU.

What will be the key changes?

- **Companies** will only have to deal with **a single national data protection authority –** in the EU country where they have their main establishment.
- Individuals will have the **right to refer all cases to their home national data protection authority**, even when their personal data is processed outside their home country.
- **EU rules will apply** to companies not established in the EU, if they offer goods or services in the EU or monitor the online behaviour of citizens.
- Increased **responsibility and accountability** for those processing personal data.
- **Unnecessary administrative burdens** such as notification requirements for companies processing personal data **will be removed**.
- **National data protection authorities will be strengthened** so they can better enforce the EU rules at home.

Can big data really revolutionise our world?

How the explosion of information and analysis will impact our lives and our privacy.

EVEN DOGS CAN HAVE A DATA TRAIL IF THEY'RE CHIPPED

IS YOUR CONNECTED CAR SPYING ON YOU?

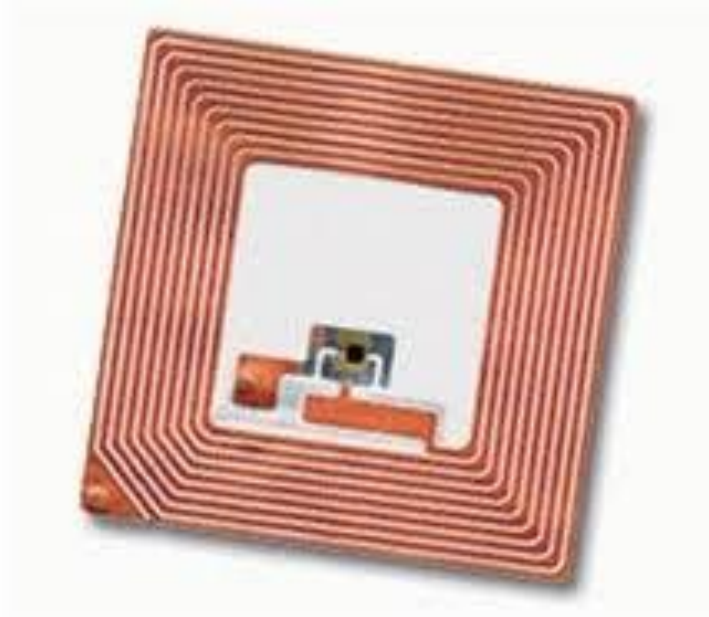
A za Oceanem:

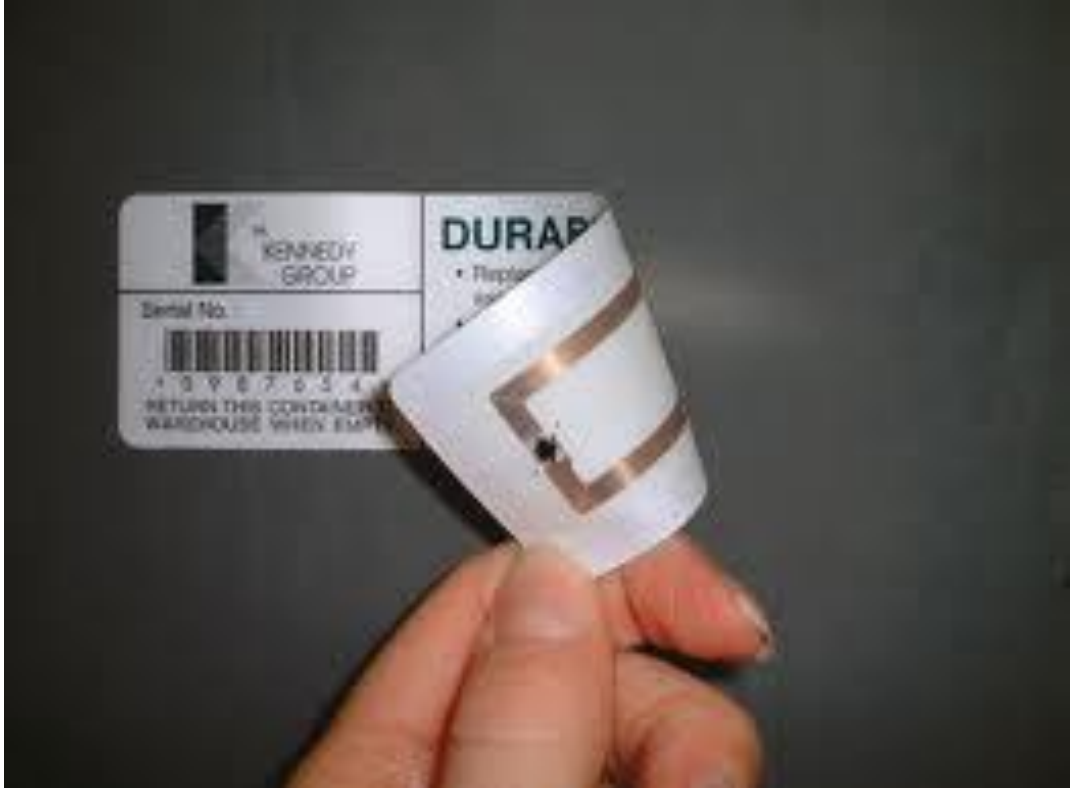
- USA Patriot Act (antyterorystyczny po 11/09)
  - wszystkie informacje gromadzone lub przetwarzane przez firmy amerykańskie oraz podmioty należące do nich podlegają kontroli amerykańskich organów państwowych i instytucji śledczych
    - Pakiet Office 365 (utajnione przekazywanie danych na żądanie – a UE wymaga powiadomienia podmiotu o ujawnieniu jego danych)
    - Google, Salesforce, Focebook etc.


Google

Inny problem:

- Technologia RFID zagraża naszej prywatności, 4.10.2011 r. (GIODO)
- *Radio-frequency identification* - Technika umożliwia odczyt, a czasami także zapis układu RFID. W zależności od konstrukcji umożliwia odczyt etykiet z odległości do kilkudziesięciu centymetrów lub kilku metrów od anteny czytnika. System odczytu umożliwia identyfikację wielu etykiet znajdujących się jednocześnie w polu odczytu. RFID przytwierdzony do przedmiotu może być jedną z form zabezpieczenia przedmiotów przed ich fałszowaniem.




KENNEDY
GROUP
Serial No.

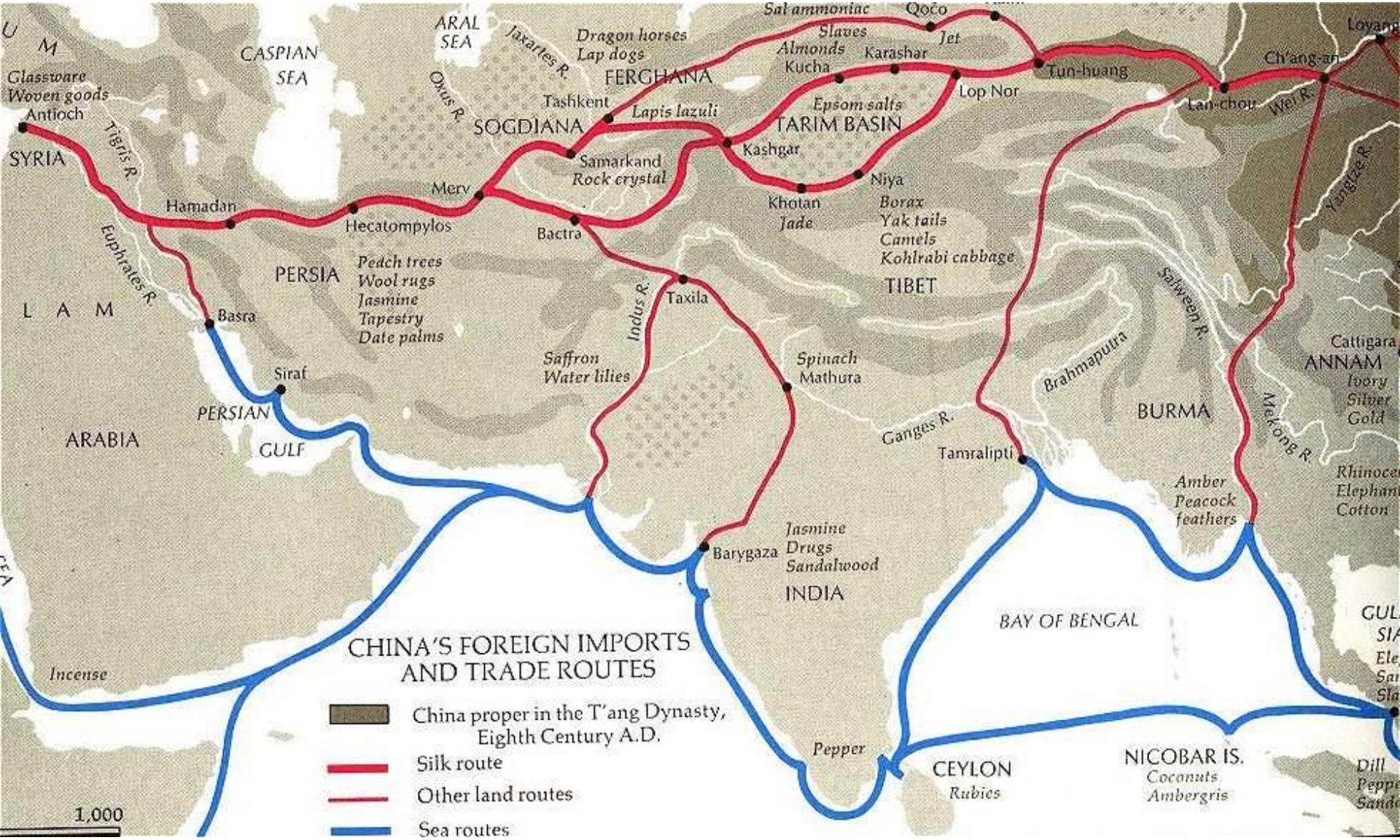
Login History

Search: 2008-08-10 Type: Time Source: AutoBan 2 Logs Limit Results: 25 Search

Search start (mm/dd/yyyy): 1 / 1 / 2004 Search end (mm/dd/yyyy): 08 / 10 / 2008

Search Results

User Name	Punkbuster GUID	IP Address	Server IP	Time
zyl.o2+	B908AC78605C0C51225175D89C8F50FF	82.17.102.152	194.153.116.165	2008-08-10 13:38:38 GMT -7
benzorevelation	AE4FE8CC7C971918502B728C6215239F	79.46.200.212	195.78.231.215	2008-08-10 13:38:37 GMT -7
Cdt._Armstrong	E0FC33CEB289BBB64F9720CB9FF0F54F	84.1.206.214	194.153.116.161	2008-08-10 13:38:36 GMT -7
miguelg7	4BCB0AB858E35A6A3AC72B6A48BE6AA3	200.138.49.165	201.48.140.157	2008-08-10 13:38:33 GMT -7
yanlizkurt_1990	4915CF291E1A1E3CFC2BC92CCE061BB1	78.177.151.84	193.200.158.105	2008-08-10 13:38:32 GMT -7
[CTN]eCHo	3A81225858B5BB774FF185BD592F15ED	89.201.147.6	62.67.42.77	2008-08-10 13:38:30 GMT -7
hollow_pl	E2138C8FAA1389668FA033024C07EDBE	89.76.246.120	194.153.116.165	2008-08-10 13:38:29 GMT -7
SpartanNix	E8C04D15D3253B7499532D9A0B0238C3	67.161.91.74	209.246.170.84	2008-08-10 13:38:29 GMT -7
Infinitize	17C1907AD991E9EFBA0D0E30AAB60E13	84.56.98.105	193.200.158.105	2008-08-10 13:38:25 GMT -7
Vanguard185	ADE294C998F762E7CFEAF0D94B12CE1F	207.250.253.177	194.153.116.174	2008-08-10 13:38:25 GMT -7
=TG=Kuba	85BC7CDE744432692AA2439E8BD55B51	87.205.252.104	194.153.116.43	2008-08-10 13:38:23 GMT -7
motherpunker	9ED3DE5C41C2DF0641CEFC8EE9B9FE46	71.218.89.115	66.55.131.112	2008-08-10 13:38:22 GMT -7
{65thinf}-CHILI_MAN	592858BB2BAFF01A31794BC00D957332	71.204.50.95	12.180.48.38	2008-08-10 13:38:20 GMT -7
DJ12341234	1514BB8E7A957D73DFB18359B8CB73D8	68.78.135.39	213.149.245.66	2008-08-10 13:38:19 GMT -7
=TG=Siuvax	A9C33B627B44A0931771306552C63DA2	89.78.225.135	194.153.116.43	2008-08-10 13:38:19 GMT -7
{SIQ-LTD.}-P3r@@	06EF6472E14356453C1DA23A8A8A53F5	194.152.16.11	93.189.2.58	2008-08-10 13:38:19 GMT -7
[BT]_Vinicius	65A34D9AEB4668E3C87CE6B594459986	189.33.40.112	200.162.238.253	2008-08-10 13:38:19 GMT -7
{UK}-Mr.Burns.CL-	383B993429BA9D1BACE8DF79EAADEA3D	82.0.127.132	66.102.113.236	2008-08-10 13:38:19 GMT -7
dyn4mic.	B990E8264033DBE63401B1E4676C89B6	87.123.243.250	212.187.247.202	2008-08-10 13:38:17 GMT -7
-snty.z!mtY^^	AC639B3629C88616A62A2EC6B9B88E98	91.37.118.175	194.153.116.95	2008-08-10 13:38:17 GMT -7
rumunszymek	847B362F043FD25C66AB270BD021CFD8	83.11.238.11	194.153.116.93	2008-08-10 13:38:16 GMT -7
CrAwL!Ng$nAkE.]FA!	72D738A512A82329FC0DCF1619ACE076	85.127.166.160	85.214.56.235	2008-08-10 13:38:11 GMT -7
-]M[-Chimera	1C38684870C3F286F227D57DABB86DC9	84.227.19.111	194.153.116.202	2008-08-10 13:38:10 GMT -7
Texasgeorgiaboi32	222F7714367DDB2198738B6D0ECC7794	98.200.228.248	12.180.48.38	2008-08-10 13:38:10 GMT -7
Nicky_Hedges	9D5348742FE42B1F8C0B95966290D940	66.43.218.72	12.180.48.34	2008-08-10 13:38:10 GMT -7


CASPIAN SEA
ARAL SEA
Jaxartes R.
Oxus R.
Tigris R.
Euphrates R.
Indus R.
Ganges R.
Brahmaputra
Salween R.
Mekong R.
Yangtze R.
Wei R.
Glassware
Woven goods
Antioch
SYRIA
Hamadan
Hecatompylos
Merv
Tashkent
SOGDIANA
FERGHANA
Dragon horses
Lap dogs
Lapis lazuli
Samarkand
Rock crystal
Bactra
Kashgar
Khotan
Jade
Niya
Borax
Yak tails
Camels
Kohlrabi cabbage
TARIM BASIN
Epsom salts
Sal ammoniac
Slaves
Almonds
Kucha
Karashar
Qoco
Jet
Lop Nor
Tun-huang
Lan-chou
Ch'ang-an
Loyang
TIBET
PERSIA
Peach trees
Wool rugs
Jasmine
Tapestry
Date palms
Basra
Siraf
PERSIAN GULF
ARABIA
Taxila
Saffron
Water lilies
Spinach
Mathura
Barygaza
Jasmine
Drugs
Sandalwood
INDIA
Tamralipti
BURMA
Amber
Peacock feathers
Cattigara
ANNAM
Ivory
Silver
Gold
BAY OF BENGAL
CEYLON
Rubies
Pepper
NICOBAR IS.
Coconuts
Ambergris
Incense
CHINA'S FOREIGN IMPORTS AND TRADE ROUTES
China proper in the T'ang Dynasty, Eighth Century A.D.
Silk route
Other land routes
Sea routes
1,000

The Underground Website Where You Can Buy Any Drug Imaginable

THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

2013.10.06

Privacy for anyone anywhere

Tails is a live operating system, that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your **privacy** and **anonymity**, and helps you to:

- **use the Internet anonymously** and **circumvent censorship**;
  all connections to the Internet are forced to go through the Tor network;
- **leave no trace** on the computer you are using unless you ask it explicitly;
- **use state-of-the-art cryptographic tools** to encrypt your files, emails and instant messaging.

Learn more about Tails.

Tails is free because **nobody should have to pay to be safe while using computers**. But Tails cannot stay alive without money and **we need your help**!

Discover who you are helping around the world when donating to Tails.

Download
Tails 1.2.3
January 14, 2015

About
Getting started...
Documentation
Help & Support
Contribute
News

Donate

News

Tails 1.2.3 is out
Posted Wed 14 Jan 2015 12:34:56 PM CET

Help porting Windows camouflage to GNOME 3.14
Posted Mon 05 Jan 2015 12:00:00 PM CET

Security

Numerous security holes in Tails 1.2.2
Posted Mon 12 Jan 2015 12:00:00 AM CET

Numerous security holes in Tails 1.2
Posted Mon 01 Dec 2014 12:00:00 AM CET

See Security for more.

amnesia, noun:
forgetfulness; loss of long-term memory.

incognito, adjective & adverb:
(of a person) having one's true identity concealed.

Tails is a live system that aims to preserve your privacy and anonymity. It helps you to use the Internet anonymously and circumvent censorship almost anywhere you go and on any computer but leaving no trace unless you ask it to explicitly.

It is a complete operating system designed to be used from a DVD, USB stick, or SD card independently of the computer's original operating system. It is Free Software and based on Debian GNU/Linux.

Tails comes with several built-in applications pre-configured with security in mind: web browser, instant messaging client, email

Tails was first released on June 23, 2009. It is the next iteration of development on Incognito, a Gentoo-based Linux distribution. Most of the financial support for its development has been provided by the Tor Project.[5] Tails has also received funding from the Debian Project, Mozilla, and the Freedom of the Press Foundation.
Laura Poitras, Glenn Greenwald, and Barton Gellman have each said that Tails was an important tool they used in their work with National Security Agency whistleblower Edward Snowden.
On July 3, 2014, German public television channel Das Erste reported that the NSA's XKeyscore surveillance system contains definitions that match persons who search for Tails using a search engine or visit the Tails website. A comment in XKeyscore's source code calls Tails "a comsec mechanism advocated by extremists on extremist forums".
On December 28, 2014, Der Spiegel published slides from an internal NSA presentation dating to June 2012 in which the NSA deemed Tails on its own as a "major threat" to its mission, and when used in conjunction with other privacy tools such as OTR, Cspace, RedPhone, and TrueCrypt was ranked as "catastrophic," leading to a "near-total loss/lack of insight to target communications, presence..."

TRUECRYPT

FREE OPEN-SOURCE

ON-THE-FLY

ENCRYPTION

TCnext

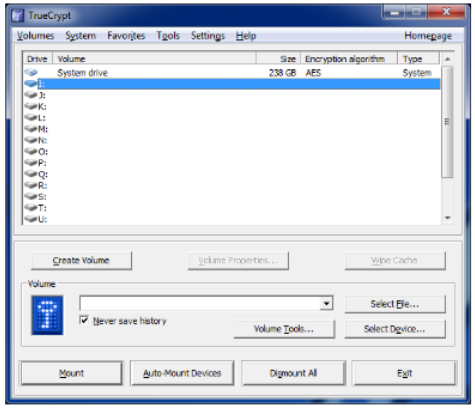
Home | Blog | Downloads | Forum | About us

TrueCrypt

must not die

TrueCrypt.ch is the gathering place for all up-to-date information. Unfortunately TrueCrypt.org really is dead. But, we organize a future.

Download Now



Located in Switzerland

If there have been legal problems with the US, the independent hosting in Switzerland will guarantee no interruption due to legal threats.

Community

We are looking for an interactive communication with the users and a bigger community effort.

Download

We offer all the downloads which are not available at TrueCrypt.org at the moment.

Non Anonymous

Anonymous development on a security relevant Project is no longer an option. The TrueCrypt.ch team will stand with their name!

In Development

Currently the news is still in flux, and we will support any efforts in reviving TrueCrypt. If other Initiatives arise we will try to support them. At the moment we want to make sure everyone who wants can continue to use TrueCrypt.

Real OSS

We put together the whole TrueCrypt Source into a github repo: feel free to clone.

Source

Tales of Unrest by Joseph Conrad

- 22 czerwca 1897 r. początek obchodów stulecia Imperium Brytyjskiego (60 rocznica wstąpienia na tron królowej Wiktorii)

"An Outpost of Progress”

- –written 1896; published in Cosmopolis, 1897

[....] After a time he found himself sitting in a chair and looking at Carlier, who lay stretched on his back. Makola was kneeling over the body.

"Is this your revolver?" asked Makola, getting up.

"Yes," said Kayerts; then he added very quickly, "He ran after me to shoot me—you saw!"

"Yes, I saw," said Makola. "There is only one revolver; where's his?"

"Don't know," whispered Kayerts in a voice that had become suddenly very faint.

The Managing Director of the Great Civilizing Company (since we know that civilization follows trade) landed first, and incontinently lost sight of the steamer. The fog down by the river was exceedingly dense; above, at the station, the bell rang unceasing and brazen.

The Director shouted loudly to the steamer:

"There is nobody down to meet us; there may be something wrong, though they are ringing. You had better come, too!"

And he began to toil up the steep bank. The captain and the engine-driver of the boat followed behind. As they scrambled up the fog thinned, and they could see their Director a good way ahead. Suddenly they saw him start forward, calling to them over his shoulder:—"Run! Run to the house! I've found one of them. Run, look for the other!"

He had found one of them! And even he, the man of varied and startling experience, was somewhat discomposed by the manner of this finding. He stood and fumbled in his pockets (for a knife) while he faced Kayerts, who was hanging by a leather strap from the cross. He had evidently climbed the grave, which was high and narrow, and after tying the end of the strap to the arm, had swung himself off. His toes were only a couple of inches above the ground; his arms hung stiffly down; he seemed to be standing rigidly at attention, but with one purple cheek playfully posed on the shoulder. And, irreverently, he was putting out a swollen tongue at his Managing Director.