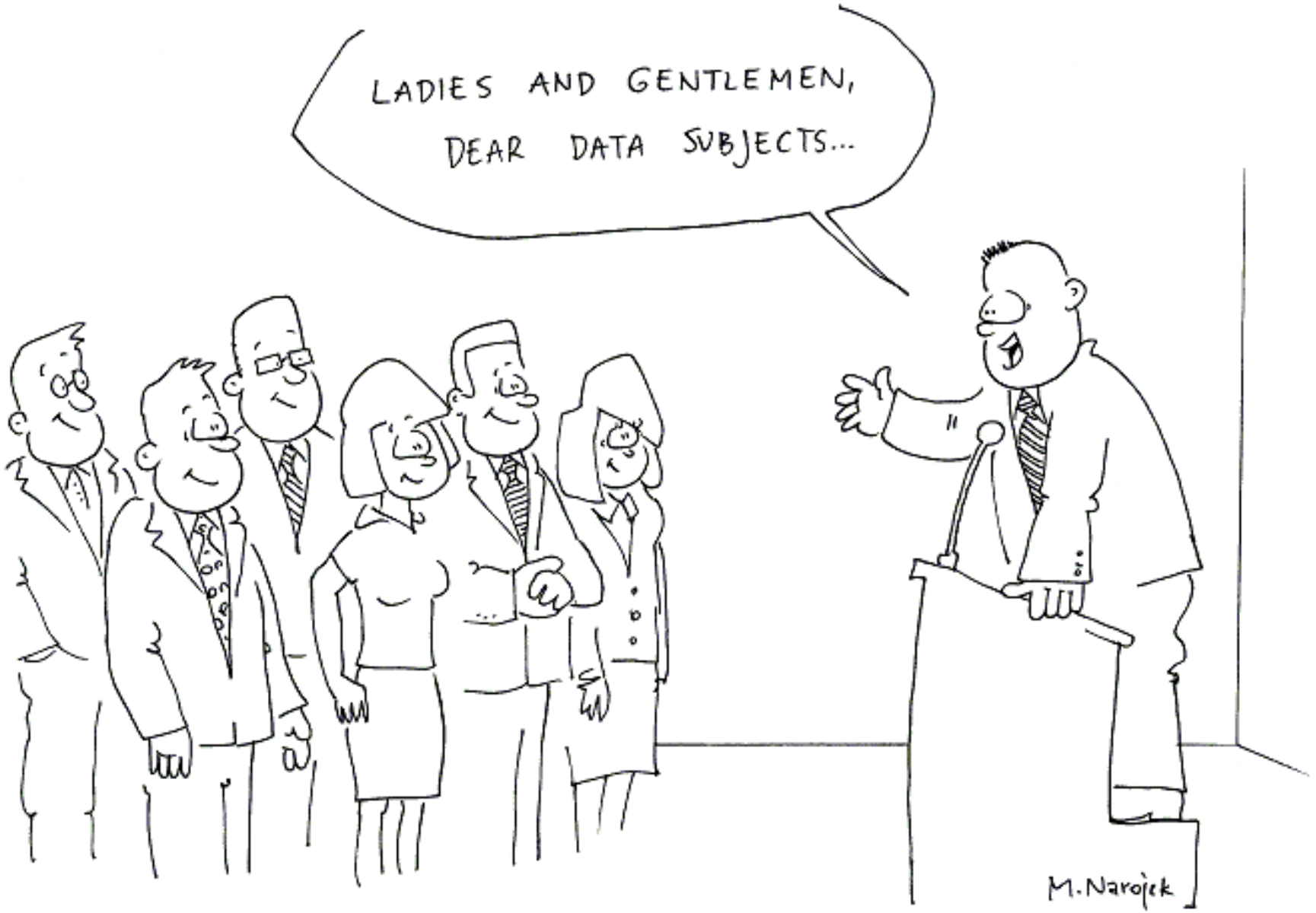
Prawo do prywatności w świecie nowych technologii informacyjnych

29/05/2018, Warszawa

Wojciech Wiewiórowski,

Zastępca Europejskiego Inspektora Ochrony Danych (EDPS)

Mazowiecki Klub Informatyka Polskiego Towarzystwa Informatycznego



Europejski Inspektor Ochrony Danych (EDPS)

EDPS jest niezależnym organem nadzorczym (odpowiednikiem GIODO dla instytucji unijnych) stworzonym dla ochrony prywatności i danych osobowych oraz wspieraniu dobrych praktyk w instytucjach unijnych.

Wiele specyficznych zadań EDPS zostało ustalonych w rozporządzeniu 45/2001.

Trzy główne obszary działań to:

Zadania nadzorcze
Zadania doradcze.
Zadania związane ze współpracą międzynarodową

Europejski Inspektor Ochrony Danych (EDPS)

- **Europejski Inspektor Ochrony Danych (EDPS)** jest niezależnym organem kontrolnym powołanym do nadzorowania przetwarzania danych przez organy, instytucje, agencje i inne jednostki Unii Europejskiej;

- Zadania:

– kontrolowanie wypełniania postanowień rozporządzenia 45/2001,
– doradzanie administratorom danych osobowych,
– doradzanie uczestnikom procesu legislacyjnego,
– współpraca z organami ochrony danych w krajach członkowskich,
– rozstrzyganie w sprawach skarg oraz inspekcje
– monitorowanie zmian technologicznych na rynku
– podwyższanie świadomości społecznej w zakresie ochrony prywatności

Konstytucja RP (art. 47)

Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Konstytucja RP (art. 51)

1. *Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.*
2. *Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.*
3. *Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.*
4. *Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.*
5. *Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.*

Prawo podstawowe w Unii Europejskiej

Artykuł 16 Traktatu o funkcjonowaniu UE (po zm. z Lizbony)

1. Każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

2. Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, określają zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraprzez Państwa Członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także zasady dotyczące swobodnego przepływu takich danych. Przestrzeganie tych zasad podlega kontroli niezależnych organów.

Zasady przyjęte na podstawie niniejszego artykułu pozostają bez uszczerbku dla zasad szczególnych przewidzianych w artykule 39 Traktatu o Unii Europejskiej.

Prywatność

15 grudnia 1890 r. przyszły sędzia amerykańskiego Sądu Najwyższego Louis Brandeis oraz Samuel Warren opublikowali w „Harvard Law Review” artykuł pt. “The Right to Privacy”, w którym postulowali uznanie nowego prawa osoby fizycznej – prawa do „bycia pozostawionym samemu sobie” (*“be let alone”*). Powodem powstania artykułu było upowszechnienie się nowej technologii – i tym samym nowego nośnika informacji – fotografii prasowej.

Prywatność

L.Brandeis, S.Warren: "The Right to Privacy", Harvard Law Review, Vol. IV, 15.12.1890, 5

That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses vi et armis. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; ***and now the right to life has come to mean the right to enjoy life, -- the right to be let alone; the right to liberty secures the exercise of extensive civil privileges;*** *and the term "property" has grown to comprise every form of possession -- intangible, as well as tangible.*

Prywatność

Prywatność posiada w terminologii znormalizowanej aż trzy definicje:

„Prawo do kontrolowania lub wpływania na to, aby informacja ich dotycząca mogła być zbierana i przechowywana oraz na to, kto może to wykonywać i komu można udostępnić tę informację.” (PN-T-20000:1994-P), przy czym definicja ta jest opatrzona komentarzem „Uwaga – Ponieważ termin jest związany z prawem osób nie może on być precyzyjny. Należy unikać używania tego terminu chyba, że kontekst odnosi się do wymagań zabezpieczania informacji.”;

„Nieingerowanie w życie prywatne osoby lub jej sprawy, jeśli ta ingerencja byłaby związana z niewłaściwym lub nielegalnym zbieraniem i wykorzystywaniem danych o tej osobie” (PN-ISO/IEC 2382-8:2001 08.01.23, PN-I-02000:2002 3.1.088);

„Prawo do nadzoru lub wpływu na to, jakie dane osobowe mogą być zbierane i przechowywane oraz komu mogą być ujawnione.” (PN-I-02000:2002 – 3.1.089, PN-T-20000:1994 – P) , przy czym definicja ta jest opatrzona komentarzem „Uwaga - Należy unikać używania tego terminu chyba, że kontekst odnosi się do wymagań zabezpieczania informacji”.

Źródło: *M. Szmit: Kilka uwag, nie tylko o dokumentach elektronicznych, [w:] Ochrona informacji niejawnych, biznesowych i danych osobowych. Materiały VII Kongresu, KSOIN, Katowice 2011, s. 193-200, ISBN 978-83-933705-0-4*

Przełomowe orzeczenie indyjskiego Sądu Najwyższego w sprawie konstytucyjności ochrony prywatności

- Wiele osób kwestionowało przepisy o karcie Aadhaar i bazie danych identyfikujących jej użytkowników. Bazę utworzono dla potrzeb objęcia wszystkich obywateli Indii jednorodnym systemem identyfikacyjnym, w którym nadano by im 12-cyfrowy numer, umożliwiający wyszukanie i zidentyfikowanie osoby. Dane w bazie obejmują między innymi skan oka, odciski palców.
to records including

- W liczącym ponad 500 stron wyroku Sąd Najwyższy stwierdził, że ochrona prywatności jest jedną z zasad konstytucji Indii, mimo że nie jest tam zapisana wprost.

Wyrok w sprawie *Sędzia K.S.Puttaswamy i inni przeciwko Indiom* z 24 sierpnia 2017 r. https://indiankanoon.org/doc/91938676/

Przełomowe orzeczenie indyjskiego Sądu Najwyższego w sprawie konstytucyjności ochrony prywatności

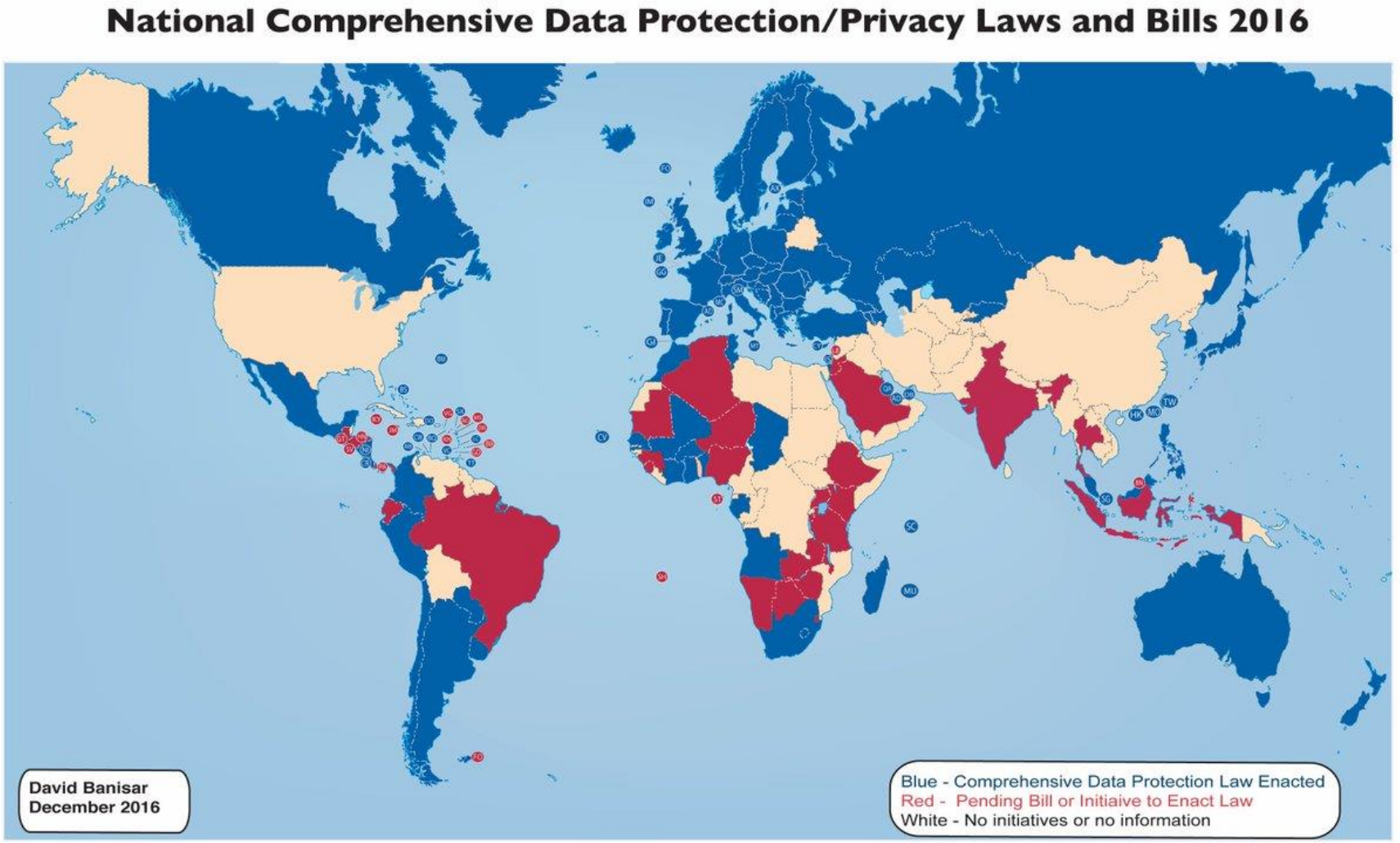
- Mimo że konstytucja Indii nie zawiera wyraźnie opisanego prawa do prywatności, prawo to jest niezbędnym elementem art. 21 ustawy zasadniczej

  (*no person can be deprived of their life or liberty without a procedure established by the law*)

- Prywatność jest podstawą (*core*) godności ludzkiej .
- Uchylono wcześniejsze sprzeczne z tym orzeczenia izb 8- i 6-osobowych.
- Wezwano rząd do wprowadzenia “silnego reżimu ochrony danych”.
- Określono, że orientacja seksualna jako część prywaności wchodzi w zakres godności ludzkiej.

Wyrok w sprawie *Sędzia K.S.Puttaswamy i inni przeciwko Indiom* z 24 sierpnia 2017 r. https://indiankanoon.org/doc/91938676/

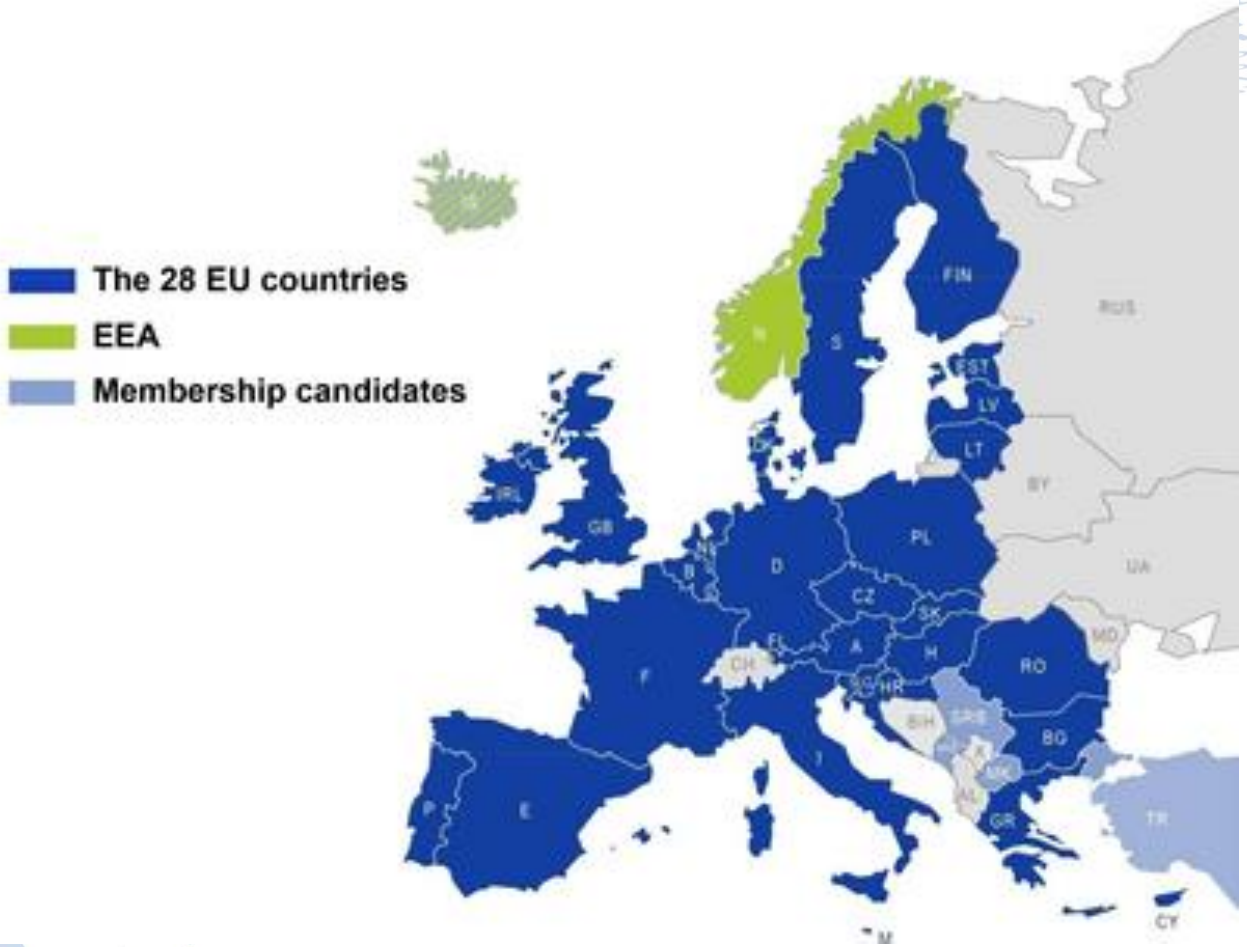
Prawo ochrony danych osobowych na świecie



13 D. Banisar, *National Comprehensive Data Protection/Privacy Laws and Bills 2016* (stan na 28,11.2016). Dostępne w SSRN: https://ssrn.com/abstract=1951416 lub http://dx.doi.org/10.2139/ssrn.1951416

Konwencja 108 – Rada Europy

Unia Europejska



Europejski Obszar Gospodarczy & EFTA

Zasięg terytorialny działania europejskiego prawa ochrony danych osobowych rozciąga się poza 28 państw członkowskich UE i obejmuje 3 kraje EFTA, które ratyfikowały traktat z Oporto i stworzyły tzw. Europejski Obszar Gospodarczy (EOG / EEA). Są to Islandia, Liechtenstein i Norwegia.

Należy pamiętać, że Transgraniczny przepływ danych do państw członkowskich EOG w celach wychodzących poza zakres rynku wewnętrznego, np. w celach dochodzeń karnych, nie podlega jednak przepisom dyrektywy o ochronie danych, a zatem nie jest objęty zasadą swobodnego przepływu danych. Jeżeli chodzi o prawo RE, konwencja nr 108 oraz protokół dodatkowy do konwencji nr 108 obejmują wszystkie obszary, chociaż umawiające się strony mogą dokonać wyłączeń. Wszystkie państwa członkowskie EOG są również stronami konwencji nr 108.

Kraje, wobec których Komisja wydała decyzje o adekwatności

Andorra - 2010/625/UE

Argentyna - 2003/490/WE

Kanada (jedynie poziom federalny) - 2002/2/WE

Szwajcaria - 2000/518/WE

Wyspy Owcze - 2010/146/UE

Guernsey - 2003/821/WE

Izrael - 2011/61/UE

Wyspa Man - 2004/411/WE
s
Nowa Zelandia - 2013/65/UE

Stany Zjednoczone – „Tarcza Prywatności” (”Privacy Shield”)

Trwają negocjacje z Japonią i Koreą Płd.

Starania rozpoczynają Maroko, Urugwaj, Wyspy Bahama

EDPS

Kraje, wobec których Komisja wydała decyzje o adekwatności

Komisja Europejska może także oceniać elementy systemu prawnego danego kraju bądź ograniczyć się do konkretnych zagadnień. Komisja dokonała na przykład ustalenia prawidłowości odnoszącego się wyłącznie do prywatnego prawa handlowego Kanady. Wydała także kilka ustaleń prawidłowości odnoszących się do przekazywania danych na podstawie umów między UE a innymi państwami. Decyzje te odnoszą się wyłącznie do jednego rodzaju przekazywania danych, np. przekazywania danych dotyczących przelotu pasażera przez linie lotnicze zagranicznym organom kontroli granicznej przy lotach z UE na niektóre lotniska zagraniczne.

Podręcznik europejskiego prawa o ochronie danych, Agencja Praw Podstawowych UE (FRA), Luksemburg 2014, Wyd. polskie, s. 143; http://giodo.gov.pl/259/id_art/7572/j/pl

Organy ochrony danych (DPA) w Unii Europejskiej

dr Edyta Bielak–Jomaa

20-LECIE PRAWA DO OCHRONY DANYCH OSOBOWYCH W POLSCE

Prawo unijne – 1995-2018

Podstawowy dokument ustanawiający obowiązujące unijne przepisy o ochronie danych, dyrektywa 95/46/WE1, został przyjęty w 1995 r. z myślą o realizacji dwóch celów: ochrony podstawowego prawa do ochrony danych oraz zagwarantowania swobodnego przepływu danych między państwami członkowskimi.

Dyrektywa 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, Dz.U. L 281 z 23.11.1995, s. 31.

Została ona uzupełniona przez szereg instrumentów przewidujących przepisy szczególne o ochronie danych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych (były trzeci filar), w tym **decyzję ramową 2008/977/WSiSW Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, Dz.U. L 350 z 30.12.2008, s. 60.**

Reforma prawa ochrony danych osobowych w Unii Europejskiej

Zdjęcie z archiumu J.P. Albrechta

Reforma prawa ochrony danych osobowych w Unii Europejskiej

Normy wywiedzione z prawa europejskiego są:

- bezpośrednio obowiązujące

- bezpośrednio stosowane

- bezpośrednio skuteczne

wertykalnie i horyzontalnie

Podstawowe pojęcia w rozporządzeniu UE (RODO)

„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;

„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;

Dane anonimowe

Dane spseudonimizowane

Dane osobowe

Anonimizacja ???

Pseudonimy

09720316017

71061302790

710613027|9|0

71|06|13|027|9|0

Podstawowe pojęcia w rozporządzeniu UE (RODO)

„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;

„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;

„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;

„podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

Zasady przetwarzania danych w rozporządzeniu UE (RODO)

1. 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; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);

e) przechowywane w formie umożliwiającej identyfikację osoby, której dane 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”).

2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

Podstawy przetwarzania danych w rozporządzeniu UE (RODO)

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą wyraziła **zgodę** na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) przetwarzanie jest **niezbędne do wykonania umowy**, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

c) przetwarzanie jest **niezbędne do wypełnienia obowiązku prawnego** ciążącego na administratorze;

d) przetwarzanie jest **niezbędne do ochrony żywotnych interesów osoby,** której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest **niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej** powierzonej administratorowi;

f) 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 podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

Dane szczególnie chronione w rozporządzeniu UE (RODO)

Zabrania się przetwarzania danych osobowych ujawniających

1. pochodzenie rasowe lub etniczne,
2. poglądy polityczne,
3. przekonania religijne lub światopoglądowe,
4. przynależność do związków zawodowych

oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej

1. danych dotyczących zdrowia,
2. seksualności lub orientacji seksualnej.

Dane szczególnie chronione w rozporządzeniu UE (RODO)

Dane szczególnie chronione można przetwarzać gdy:

a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, […];

b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym […];

c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

Dane szczególnie chronione w rozporządzeniu UE (RODO)

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, […];

h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego […];

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego[…];

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

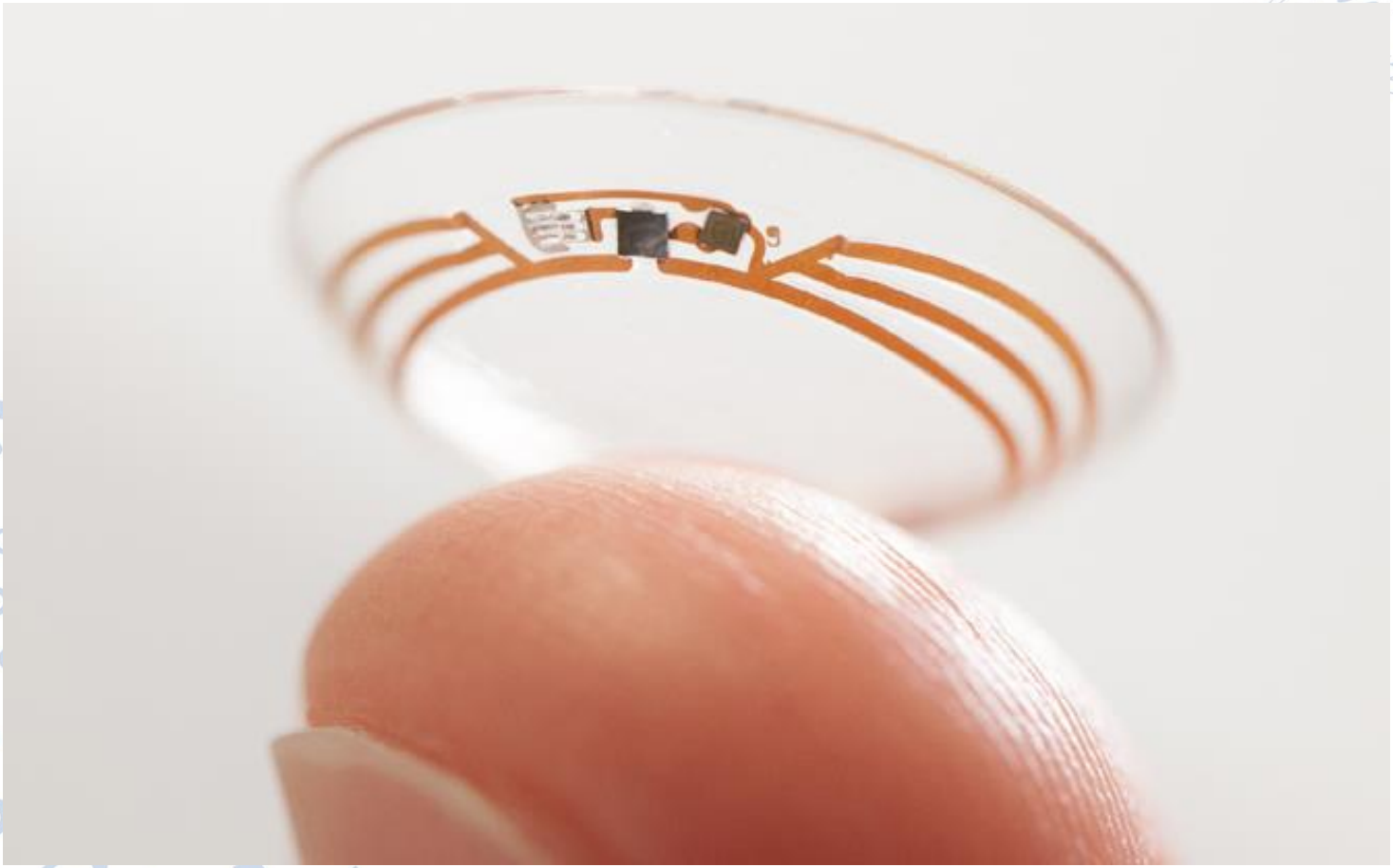
Dane szczególnie chronione w rozporządzeniu UE (RODO)

Dane osobowe, o których mowa w ust. 1, mogą być przetwarzane do celów, o których mowa w ust. 2 lit. h), jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.

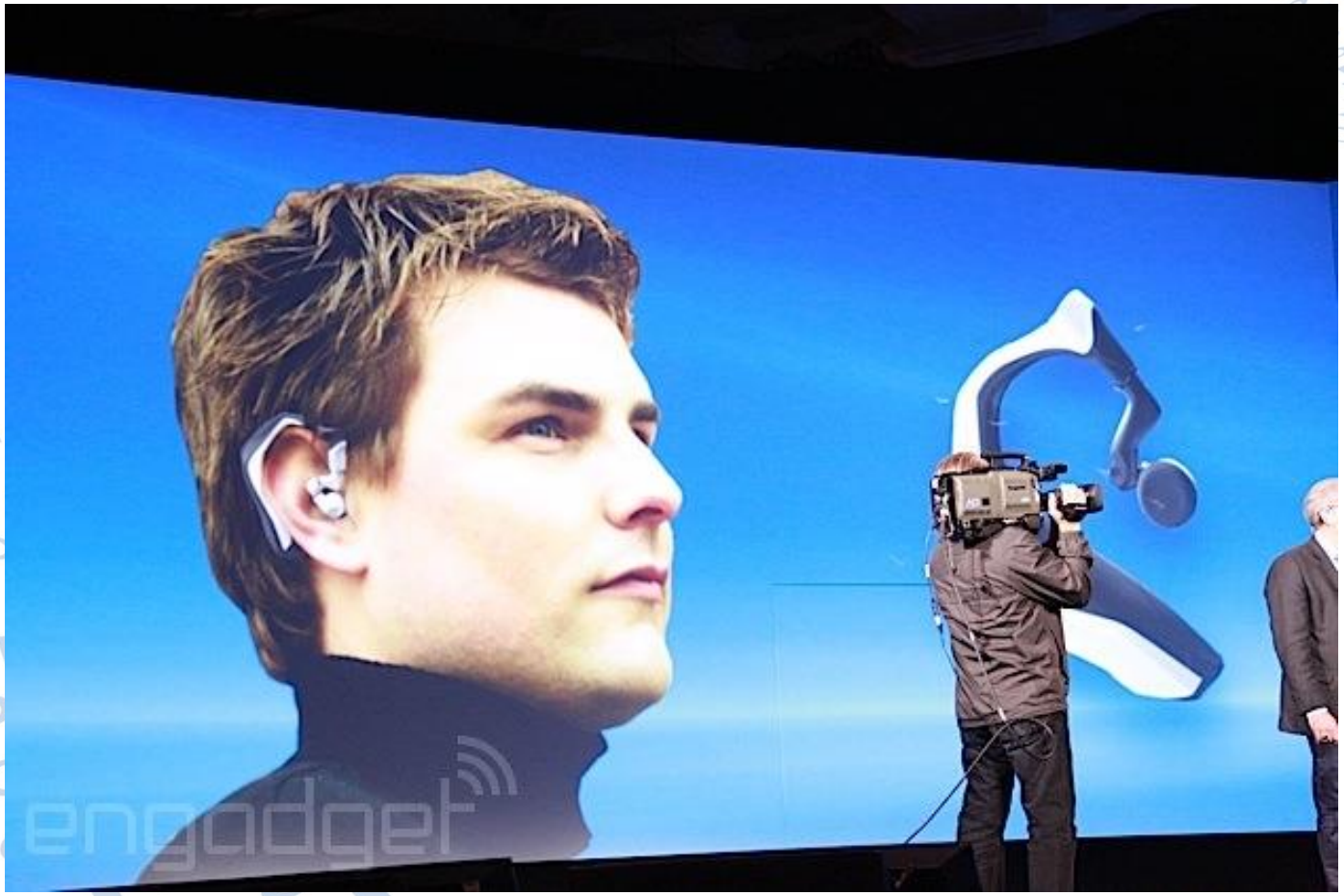
Państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.

Im więcej danych
tym większa odpowiedzialność

Wearables



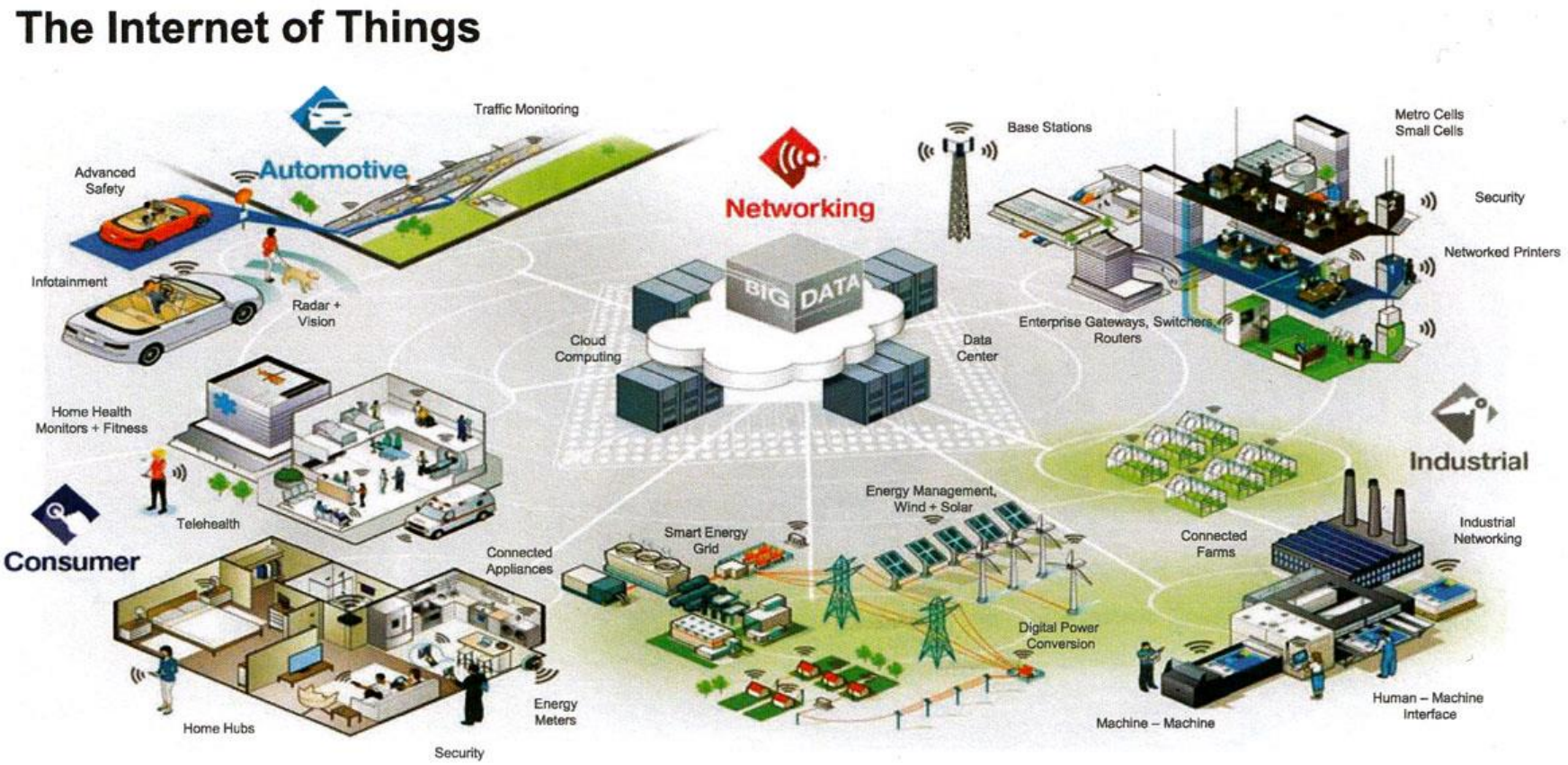
Wearables



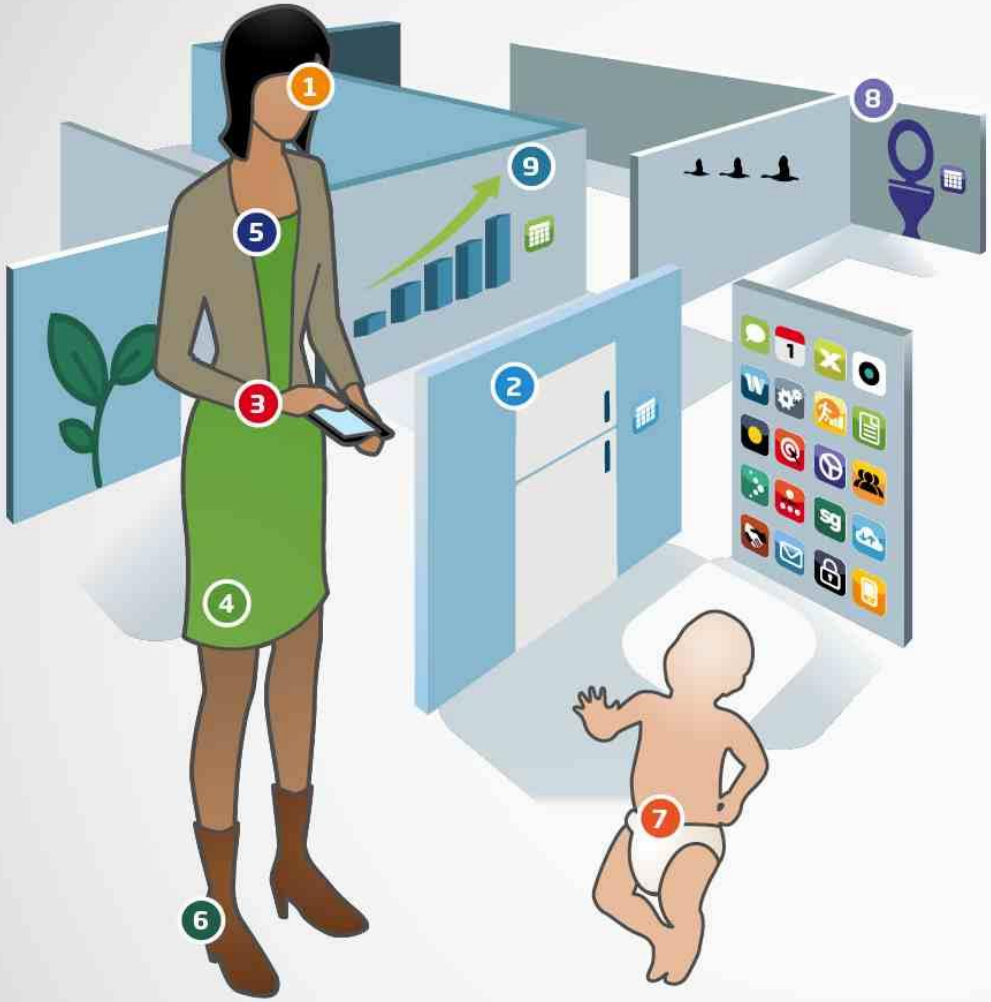
Wearables

Wearables & Quantified Self (Lifelogging)

Internet Rzeczy



Mobile health in **2024**



1. Contact lenses

A microscopic camera in the lens takes pictures of the **retina** and matches these to past cases, identifying early symptoms of **diabetic retinopathy**

Fact
1% of global blindness can be attributed to diabetes. Approximately 4,200 people in England are blind due to diabetic retinopathy

2. Fridge

The fridge monitors the **digestive system**: drinks consumed (thirst); vitamin consumption (**deficiencies**); calories/sugar consumption (insulin levels)

Fact
Diabetes is set to cost the NHS £16.9 billion by 2035/6

3. Artificial pancreas

Mini artificial **pancreas** to detect irregular **blood sugar** levels and injects insulin when necessary

Fact
Worldwide in 2013, 382 million people had diabetes; by 2035 this is projected to rise to 592 million

4. Clothes

Smart fibres in all clothes sense a rash or skin condition appearing, signalling the possible onset of diseases such as **skin cancer**

Fact
There are currently almost 13,000 new cases of skin cancer diagnosed each year in the UK

5. Thermometer patch

An electronic stick-on "tattoo", half the width of a human hair in size that detects precise **temperature changes** around the area of skin where it is placed, tracking **heat flow** through the bloodstream. This indicates **cardiovascular activity**

Fact
The number of people who die from cardiovascular diseases, mainly from heart disease and stroke, will increase to 23.3 million by 2030

6. Shoes and socks

Shoes and socks track movement of **feet**, detect when you are too sedentary and update you on **fitness** goals, as well as monitoring your **weight**

Fact
Physical inactivity costs the NHS £900 million annually

7. Nappies

Smart nappies monitor children's **sleeping patterns** and **body temperature** for symptoms of illness such as **dehydration**

Fact
Approximately 440,000 children around the world have diabetes with 70,000 new cases diagnosed each year

8. Toilet

The smart toilet monitors the **liver** and **kidney** by measuring the frequency and amount of urine passed, analysing for **glucose levels**, **dehydration**, **infection** and kidney problems. It also alerts for high **blood pressure**, a symptom of heart disease

Fact
Coronary Heart Disease is the UK's biggest killer with 82,000 deaths annually. Globally, more people die from cardiovascular disease than any other cause

9. Monitoring

Continuous **data collection** and instant **reporting** of fitness mean that prevention of disease can be **incentivised** with rewards for positive behaviour – the "gamification" of healthcare, driving **positive behaviour change**

Fact
Obesity could cost the NHS £9.7 billion more by 2050

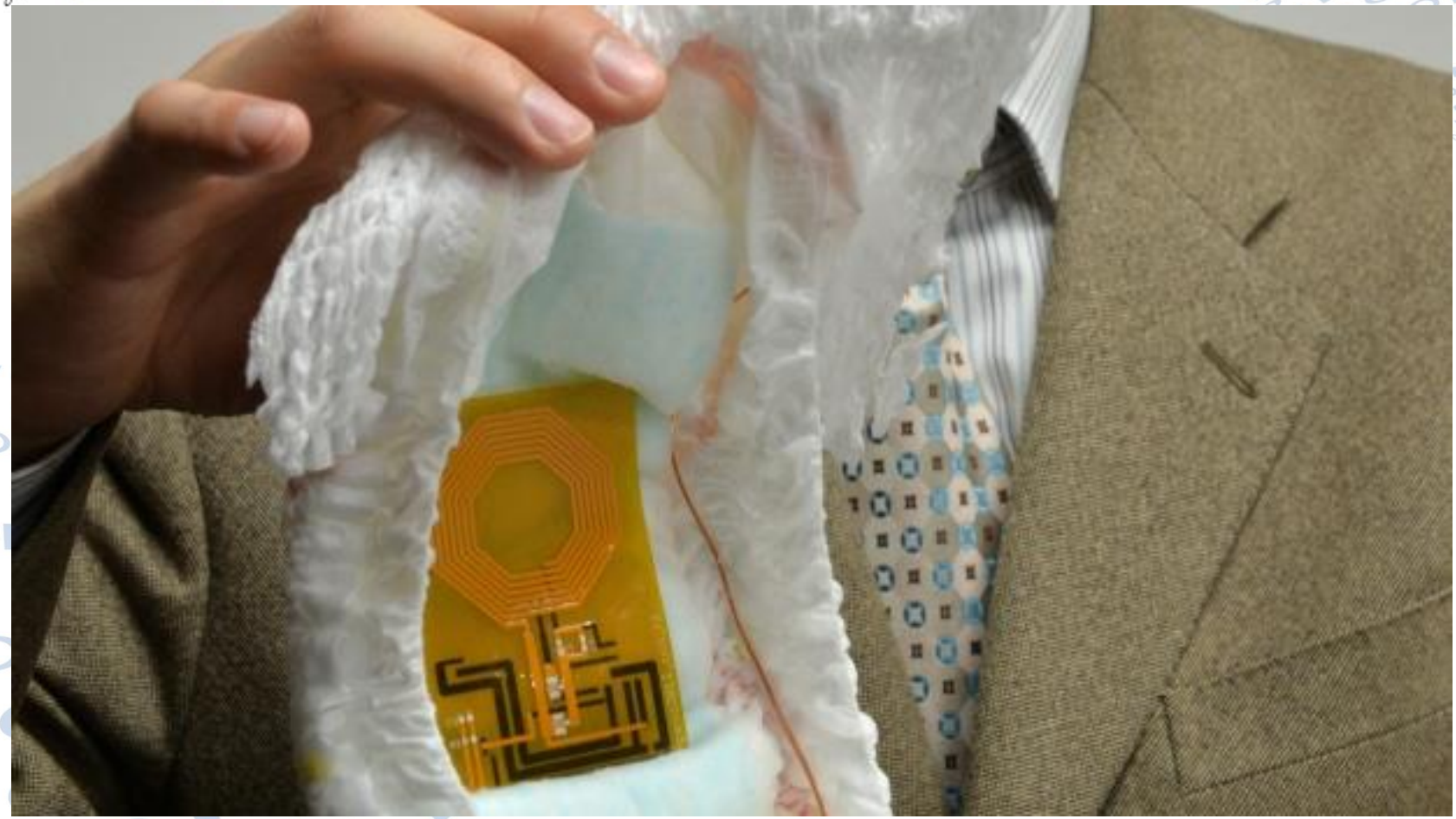
Bupa

www.bupa.com/mhealth

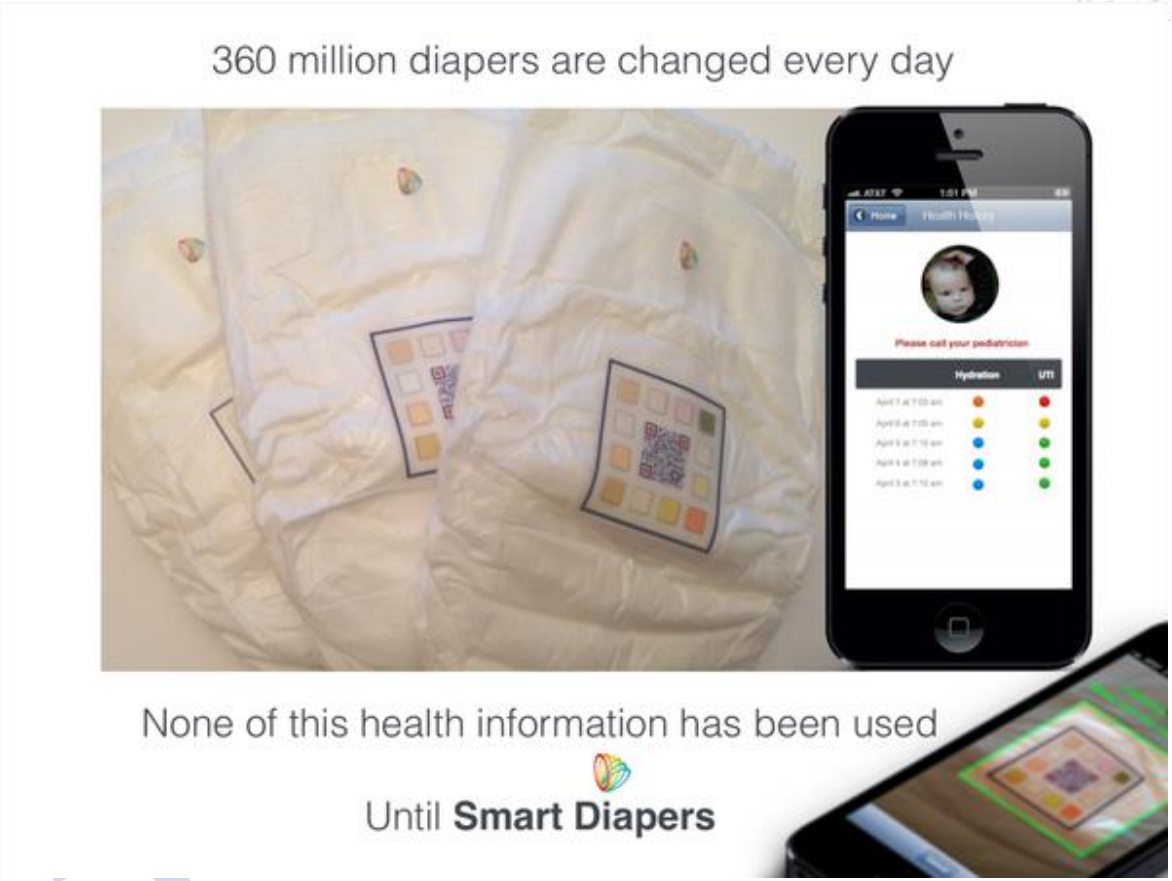
@Bupa BupaHealth Bupa

1: 'Diabetes in the UK 2012', Diabetes UK, **2:** Study in the journal 'Diabetic Medicine', Diabetes UK website, **3:** International Diabetes Federation, **4:** NHS Online, **5:** 'Global atlas on cardiovascular disease prevention and control', World Health Organization, 2011, **6:** British Heart Foundation, 'Physical Activity statistics 2012', **7:** The International Diabetes Federation, **8:** NHS online, **9:** 'Assessing the costs to the NHS associated with alcohol and obesity in Wales', Welsh Assembly Government Social Research, 2011

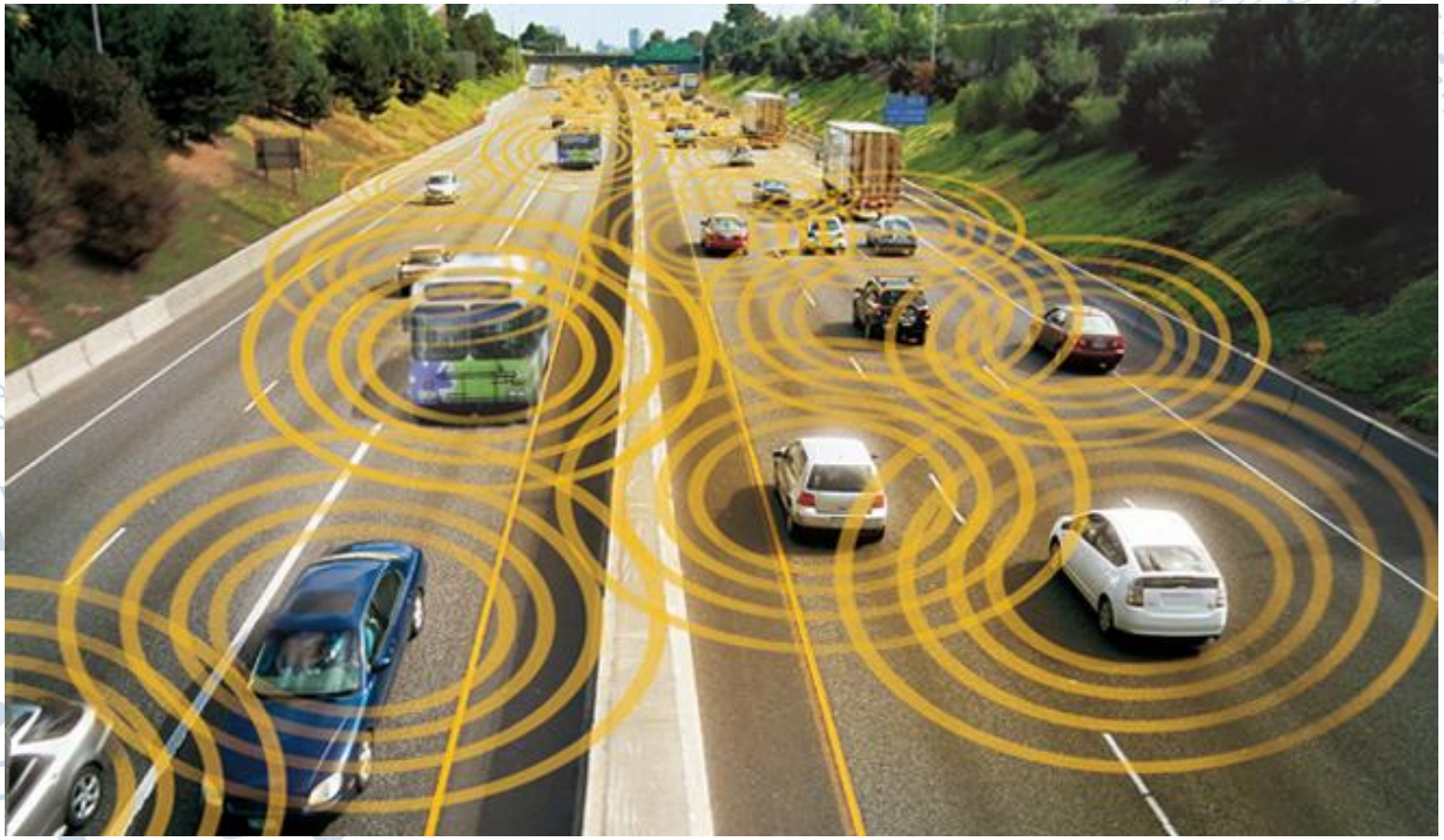
Inteligentne pieluszki



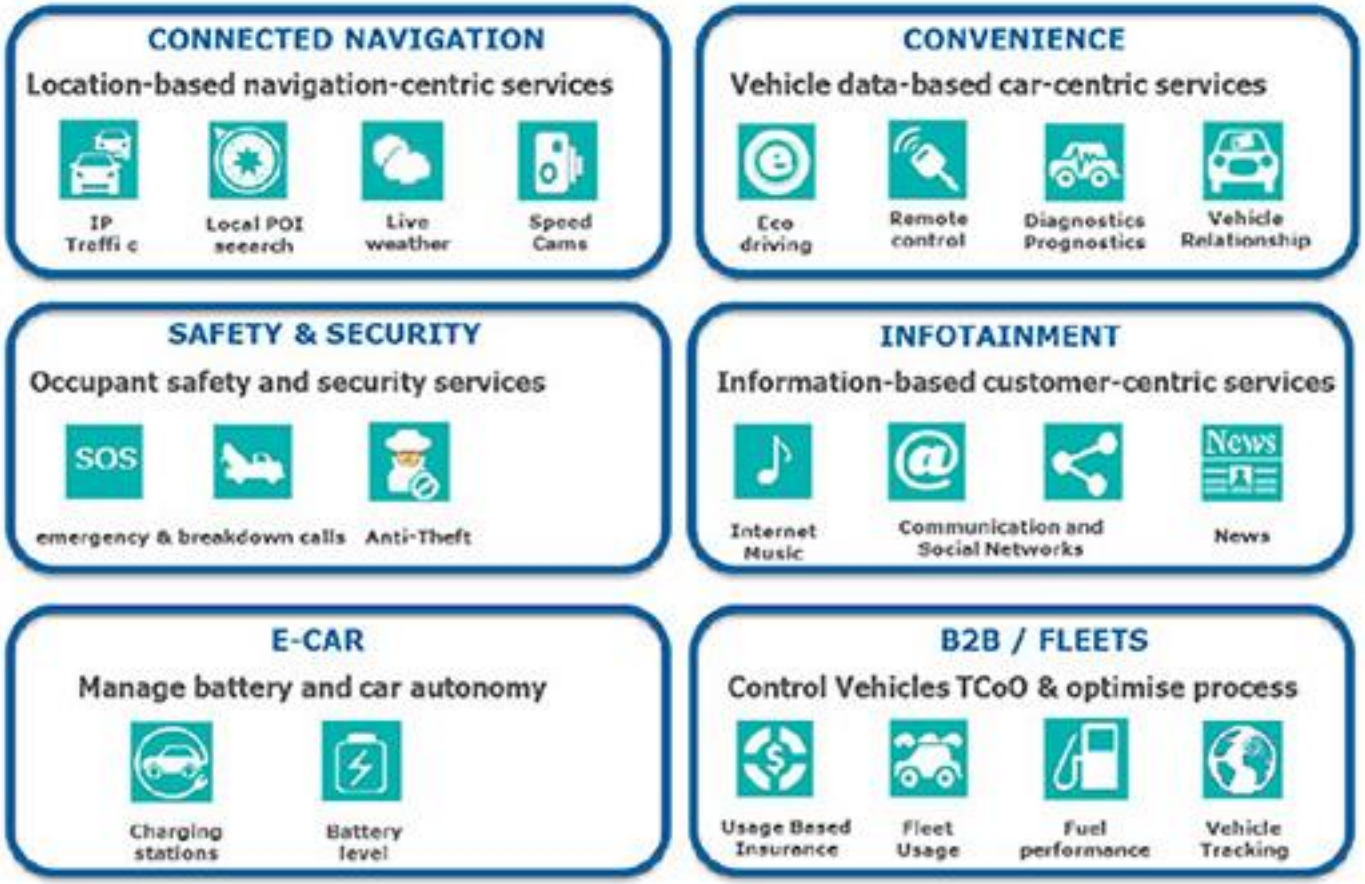
Inteligentne pieluszki



Połączone samochody

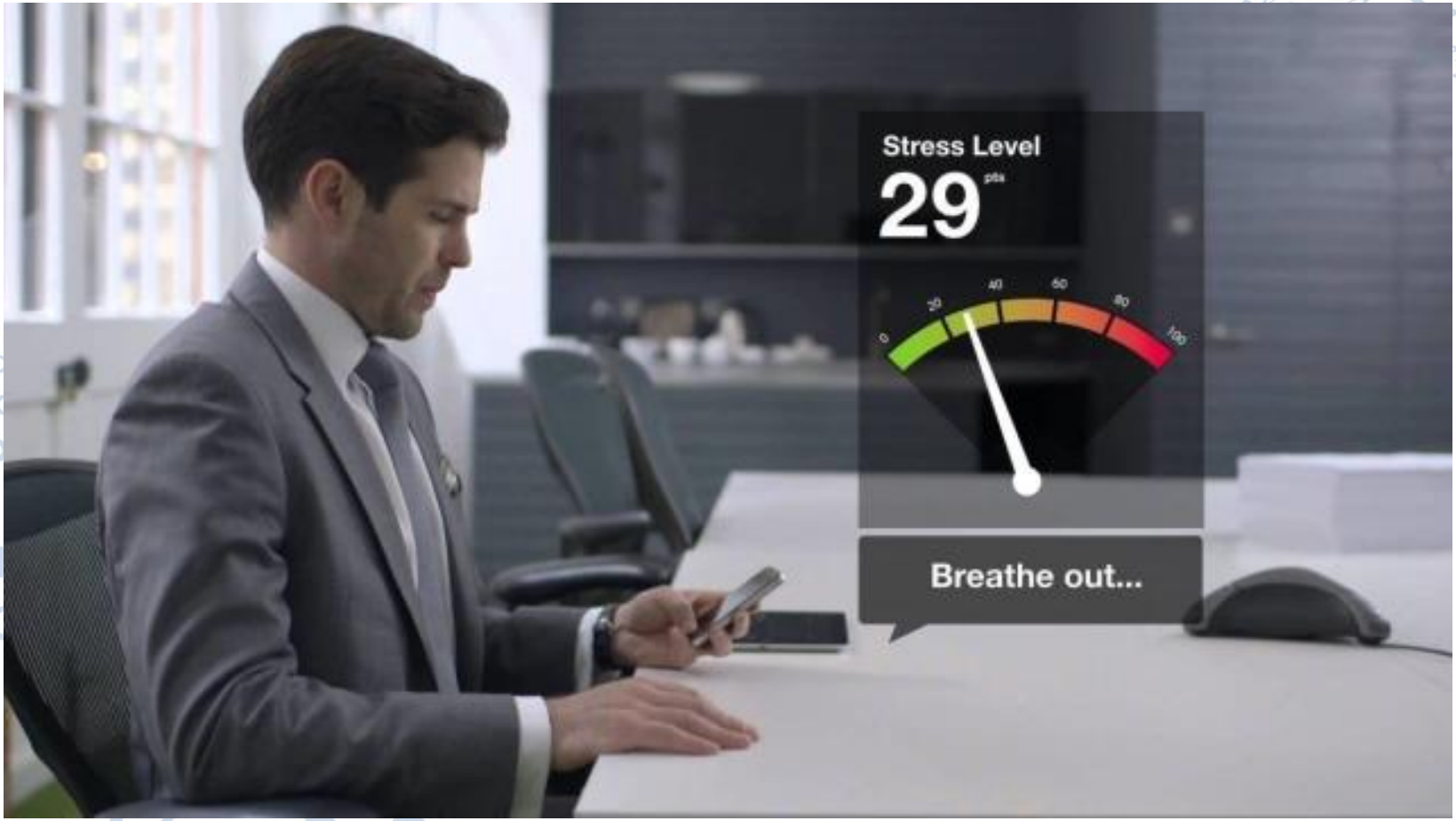


Połączone samochody



Atos, Connected Cars: *http://uk.atos.net/en-uk/home/we-do/business-integration-solutions/smart-mobility/connected-cars.html*

Jak się czuje Twój pracownik ?



Sztuczna inteligencja i robotyka a ochrona danych osobowych

Sztuczna inteligencja i robotyka a ochrona danych osobowych

Transparency.

Unless individuals are provided with appropriate information and control, they '*will be subject to decisions that they do not understand and have no control over*'.

Having that appropriate information can be complicated by two different factors:

- organisations claiming secrecy over *how* data is processed on grounds of trade secrets
- intrinsic difficulty on providing an explanation for a prediction when that prediction is based on an artificial intelligence algorithm that has been created using machined learning: the logic behind the machine reasoning may not be *expressible* in human terms.

Sztuczna inteligencja i robotyka a ochrona danych osobowych

AlphaGo is beating *go* player Lee Sedol
"Hand of God" 2/37 v 4/78

"W drugiej partii maszyna Google wykonała ruch, którego żaden człowiek by nie wymyślił. To było piękne. Świat patrzył na rozegranie pokazujące doskonale jak niesamowicie potężne i wręcz tajemne są możliwości współczesnej sztucznej inteligencji.

Tymczasem w partii czwartej człowiek wykonał ruch, którego żadna maszyna nigdy by się nie spodziewała. I to też było piękne. Zaiste tak piękne jak ruch ze strony maszyny – ani mniej ani więcej. Pokazało to, że choć maszyny mają swe chwile geniuszu, człowiek nie zatracił możliwości osiągnięcia swych transcendentnych momentów. Wydaje się, że w kolejnych latach, gdy człowiek będzie pracował z tymi maszynami, nasz geniusz będzie rósł wspólnie z geniuszem naszych dzieł."

Geordie Wood, *In Two Moves, AlphaGo and Lee Sedol Redefined the Future*, WIRED [tłum. własne] March 13th, 2016 *https://www.wired.com/2016/03/two-moves-alphago-lee-sedol-redefined-future/*

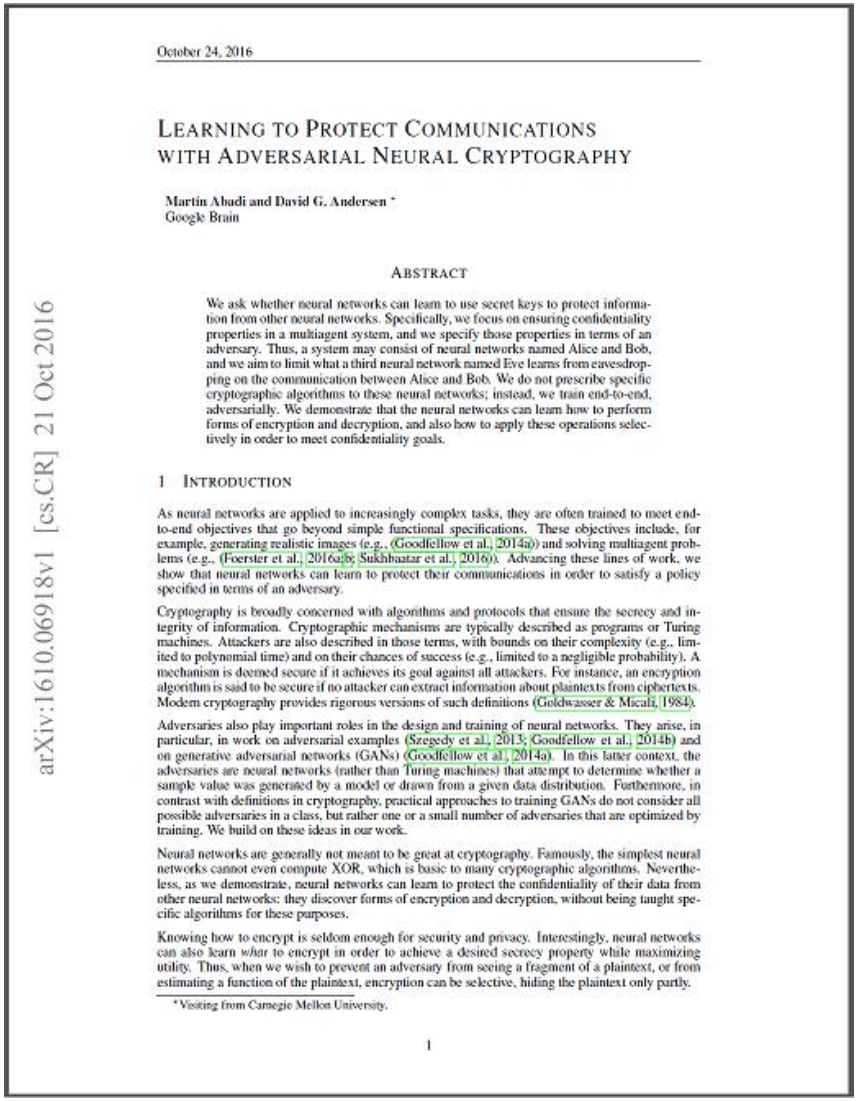
Sztuczna inteligencja i robotyka a ochrona danych osobowych

W maju 2016 r. kancelaria prawnicza BakerHostetler z centralą w Cleveland w stanie Ohio poinformowała, że w stulecie swego istnienia postanowiła jako pierwsza globalna firma prawnicza „zatrudnić" system sztucznej inteligencji Ross jako „adwokata" w swym biurze dla wspierania działu zajmującego się postępowaniami upadłościowymi. Ross jest systemem opartym na rozwijanych od kilku lat przez IBM rozwiązaniach platformy Watson, oferującej samouczące się i aktywnie korzystające z rozproszonych baz wiedzy narzędzia.

Ross został stworzony w celu odczytywania zadawanych w języku naturalnym kwestii, proponowania hipotez odpowiedzi, wyszukiwania i generowania odpowiedzi opatrzonych odwołaniami do literatury i zasobów sieciowych, by wspierać proponowane rozumowanie.

Z założenia Ross na bieżąco obserwuje zmiany w prawie, uzupełniając to informacjami z rozproszonych baz dotyczących orzecznictwa sądowego. Istotną funkcjonalnością systemu jest ograniczanie liczby rezultatów odpowiedzi według wbudowanego, ale samouczącego się algorytmu. Oznacza to, że z tysięcy możliwych odpowiedzi Ross wybierze te, które sam uzna za najważniejsze.

Sztuczna inteligencja i robotyka a ochrona danych osobowych



October 24, 2016

LEARNING TO PROTECT COMMUNICATIONS WITH ADVERSARIAL NEURAL CRYPTOGRAPHY

Martín Abadi and David G. Andersen *
Google Brain

ABSTRACT

We ask whether neural networks can learn to use secret keys to protect information from other neural networks. Specifically, we focus on ensuring confidentiality properties in a multiagent system, and we specify those properties in terms of an adversary. Thus, a system may consist of neural networks named Alice and Bob, and we aim to limit what a third neural network named Eve learns from eavesdropping on the communication between Alice and Bob. We do not prescribe specific cryptographic algorithms to these neural networks; instead, we train end-to-end, adversarially. We demonstrate that the neural networks can learn how to perform forms of encryption and decryption, and also how to apply these operations selectively in order to meet confidentiality goals.

1 INTRODUCTION

As neural networks are applied to increasingly complex tasks, they are often trained to meet end-to-end objectives that go beyond simple functional specifications. These objectives include, for example, generating realistic images (e.g., (Goodfellow et al., 2014a)) and solving multiagent problems (e.g., (Foerster et al., 2016a;b; Sukhbaatar et al., 2016)). Advancing these lines of work, we show that neural networks can learn to protect their communications in order to satisfy a policy specified in terms of an adversary.

Cryptography is broadly concerned with algorithms and protocols that ensure the secrecy and integrity of information. Cryptographic mechanisms are typically described as programs or Turing machines. Attackers are also described in those terms, with bounds on their complexity (e.g., limited to polynomial time) and on their chances of success (e.g., limited to a negligible probability). A mechanism is deemed secure if it achieves its goal against all attackers. For instance, an encryption algorithm is said to be secure if no attacker can extract information about plaintexts from ciphertexts. Modern cryptography provides rigorous versions of such definitions (Goldwasser & Micali, 1984).

Adversaries also play important roles in the design and training of neural networks. They arise, in particular, in work on adversarial examples (Szegedy et al., 2013; Goodfellow et al., 2014b) and on generative adversarial networks (GANs) (Goodfellow et al., 2014a). In this latter context, the adversaries are neural networks (rather than Turing machines) that attempt to determine whether a sample value was generated by a model or drawn from a given data distribution. Furthermore, in contrast with definitions in cryptography, practical approaches to training GANs do not consider all possible adversaries in a class, but rather one or a small number of adversaries that are optimized by training. We build on these ideas in our work.

Neural networks are generally not meant to be great at cryptography. Famously, the simplest neural networks cannot even compute XOR, which is basic to many cryptographic algorithms. Nevertheless, as we demonstrate, neural networks can learn to protect the confidentiality of their data from other neural networks: they discover forms of encryption and decryption, without being taught specific algorithms for these purposes.

Knowing how to encrypt is seldom enough for security and privacy. Interestingly, neural networks can also learn *what* to encrypt in order to achieve a desired secrecy property while maximizing utility. Thus, when we wish to prevent an adversary from seeing a fragment of a plaintext, or from estimating a function of the plaintext, encryption can be selective, hiding the plaintext only partly.

*Visiting from Carnegie Mellon University.

1

Govs want to regulate strong cryptography ?

Uhm ...

How strong crypto do they mean ?

PROFILOWANIE

PROFILOWANIE

PROFILOWANIE

„Profil” oznacza zestaw danych charakteryzują
kategorię osób, który ma zostać zastosowany
odniesieniu do danej osoby.

„Tworzenie profili” oznacza automatyczną
technikę przetwarzania danych polegającą
na przypisaniu danej osobie „profilu” w celu
podejmowania dotyczących jej decyzji
bądź analizy lub przewidywania jej preferencji,
zachowań i postaw.

PROFILOWANIE

Tworzenie profili, wg Grupy art. 29
Istnieją dwa podstawowe podejścia do tworzenia profili użytkowników:

***i) Profile* predykcyjne** tworzy się w drodze wnioskowania na podstawie obserwacji indywidualnego i zbiorowego zachowania użytkowników w czasie, w szczególności poprzez monitorowanie odwiedzanych stron oraz reklam, które użytkownik wyświetla, lub na które klika.

ii) ***Profile* jawne** tworzy się na podstawie danych osobowych przekazywanych w ramach usługi sieciowej przez same osoby, których dane dotyczą, np. podczas rejestracji. Wspomniane podejścia można łączyć. Ponadto profile predykcyjne mogą stać się jawne później, kiedy osoba, której dotyczą dane utworzy dane logowania dla danej strony internetowej.

Patrz: Opinia Grupy art. 29 nr 2/2010 w sprawie internetowej reklamy behawioralnej przyjęta dnia 22 czerwca 2010 r., pkt 2.3., str. 8

PROFILOWANIE

CELE PROFILOWANIA

- używanie tej metody ma trzy zasadnicze cele:

1. uzyskanie społecznej i psychologicznej oceny klienta
2. uzyskanie informacji o materialno - społecznym statusie klienta
3. opracowanie sugestii i strategii dla prowadzących działania marketingowe

Takie wyjaśnienie można by bez kłopotu zastosować do profilowania dla celów marketingowych, gdyby nie fakt, że …..

….. jest to teza z książki ekspertów FBI nt. profilowania zbrodniarzy, w której słowo „przestępca" zastąpiono słowem „klient", a „śledztwo" „działaniami marketingowymi" ☺

Patrz: Holmes, R. M., & Holmes, S. T. : Profiling Violent Crimes: An Investigative Tool , Wyd. IV ,Thousand Oaks: Sage Publications, Inc. 2008

Wydział Prawa i Administracji Uniwersytetu Gdańskiego - strona pracownika: dr Wojciech Rafał Wi - Windows Internet Explorer

http://www.prawo.ug.edu.pl/pracownik/wojciechrafalwiewiorowski.html

Windows Live wiewiorowski Co nowego Profil Poczta Fotografie Kalendarz MSN Udostępnianie

Ulubione Sugerowane witryny Galeria obiektów Web ...

Wydział Prawa i Administracji Uniwersytetu Gdań...

Strona główna Wydziału | Adresy i telefony na Wydziale | Sprawdź pocztę | Mapa serwisu | Pytar

UNIWERSYTET GDAŃSKI do strony głównej UG

WYDZIAŁ PRAWA I ADMINISTRACJI

Źródło rzetelnej wiedzy

rona główna WPiA
tedry i Zakłady

acownicy:
Adamczak Wojciech
Adamczak-Retecka Monika
Adamowicz Magdalena
Adrych Izabela
Amielańczyk Krzysztof
Bagińska Ewa
Balmas Agnieszka
Balwicka-Szczyrba Małgorzata
Barczewski Maciej
Bąkowski Tomasz
Błędzki Piotr
Bogusz Mariusz
Bojanowski Eugeniusz
Bojar-Fijałkowski Tomasz
Bosnegeanu Teresa
Brodecka-Chamera Aleksandra
Brodecki Zdzisław
Brzeski Marcin
Cern Grażyna
Ceynowa Maria
Chomiak Roman
Chyc Paweł
Ciechanowicz-McLean Janina
Cieslewicz Nicholas
Cieślak Wojciech
Ciszewski Jerzy
Cora Łukasz
Cora Stanisław

dr Wojciech Rafał Wiewiórowski

Pracownia Informatyki Prawniczej

Adiunkt

Pokój: 1031 (sekretariat: 4023)
Email: wiewiorowski@o2.pl (sekretariat: sekretariat03@prawo.univ.gda.pl)
Urlop bezpłatny w roku akademickim 2010-11

Generalny Inspektor Ochrony Danych Osobowych

- Sekretarz Komitetu Rady Ministrów do spraw Informatyzacji i Łączności (2008-2010);
- Dyrektor Departamentu Informatyzacji w Ministerstwie Spraw Wewnętrznych i Administracji (2008-2010);
- Mediator Sądu Polubownego do spraw Domen Internetowych przy Polskiej Izbie Informatyki i Telekomunikacji ;
- Członek Rady Programowej kwartalnika "Czas Informacji - Prawo nowych technologii. Informacja w administracji i gospodarce"
- Członek Rady Programowej "Kwartalnika Naukowego Prawo Mediów Elektronicznych "
- Członek Komitetu ds. rozwiązań interoperacyjnych dla europejskich administracji publicznych przy Komisji Europejskiej [Komitet ISA] (2008-2010)
- Członek Rady Archiwalnej przy Ministrze Kultury i Dziedzictwa Narodowego (2010)

Internet | Tryb chroniony: włączony 100%

Stary układ stron Logowanie i rejestracja

Historia i autorzy Szukaj

2010

Wojciech Wiewiórowski

Data i miejsce urodzenia	13 czerwca 1971 Łęczyca
Generalny Inspektor Ochrony Danych Osobowych	
Okres urzędowania	od 4 sierpnia 2010
Poprzednik	Michał Serzycki

lizuje się
e
a i

jno
- Wolters

rmatyzacji w jego gabinecie politycznym. Wojciech
remiera i ministra spraw wewnętrznych i administracji
stra Spraw Wewnętrznych i Administracji, Komisji
yzacji Ministerstwa Spraw Wewnętrznych i
go Stowarzyszenia Prawa Europejskiego[2][4].

włączony 100%

Wojciech Rafał Wiewiórowski - Windows Internet Explorer

http://www.goldenline.pl/wojciech-rafal-wiewiorowski

Windows Live wiewiorowski Co nowego Profil Poczta

Ulubione Sugerowane witryny Galeria obiektów Web ...

Wojciech Rafał Wiewiórowski

GoldenLine Strona główna Praca

To nie jest **Wojciech Rafał**, którego szukasz? Sz

offline

Wojciech Rafał
Generalny Inspektor Oc
Uniwersytet Gdański

Wyślij wiadomość Do

Miejscowość: Gdańsk , po
Strona www: Biogram nau Gdańskiego
Branże: Administracja Prawo

Doświadczenie i referencje

Firma: **Biuro Generalnego Inspektora Ochron** (od 2010-08)
Stanowisko: Generalny Inspektor Ochrony Danych Osob

Gotowe

22:11
2011-03-20

Wojciech Wiewiórowski - Windows Internet Explorer

http://www.facebook.com/home.php#!/profile.php?id=1393597088

Windows Live wiewiorowski Co nowego Profil Poczta Fotografie Kalendarz MSN Udostępnianie Zarejestruj się

Ulubione Sugerowane witryny Galeria obiektów Web ...

Wojciech Wiewiórowski

Strona Bezpieczeństwo Narzędzia

facebook Search Home Profile Account

Wojciech Wiewiórowski

Edit Profile

Inspector General for Personal Data Protection at Bureau of the Inspector General for Personal Data Protection Studied Law (PhD in constitutional law) at University of Gdańsk Lives in Warsaw, Poland Married From Gdansk, Poland Born on 13 June 1971 Add languages you know Edit Profile

Unread updates

Dane osobowe a usługi FinTech

Dane osobowe a usługi FinTech

FinTech today comprises five major areas:

(1) Finance and investment such as **alternative financing mechanisms**, particularly crowdfunding and P2P lending, but also robo-advisory services;

(2) Operations and risk management to build up better compliance systems (i.e. RegTech);

(3) Payments and infrastructure, such as internet and mobile payment systems, and infrastructure for securities trading and settlement and for over-the-counter (OTC) derivatives trading;

(4) Data security and monetisation to enhance the efficiency and availability of financial services (through the use of ‘big data’), to better exploit the monetary value of data, and to tackle cybercrime and espionage;

(5) Customer interface such as online and mobile financial services.

Dane osobowe a usługi FinTech

Social trading networks

eToro

Dane osobowe a usługi FinTech

Smart Contracts

Dane osobowe a usługi FinTech

Decentralized autonomous organization

DASH

digix

Dane osobowe a usługi FinTech

Robo-advisory

PERSONAL CAPITAL

wealthfront

Betterment

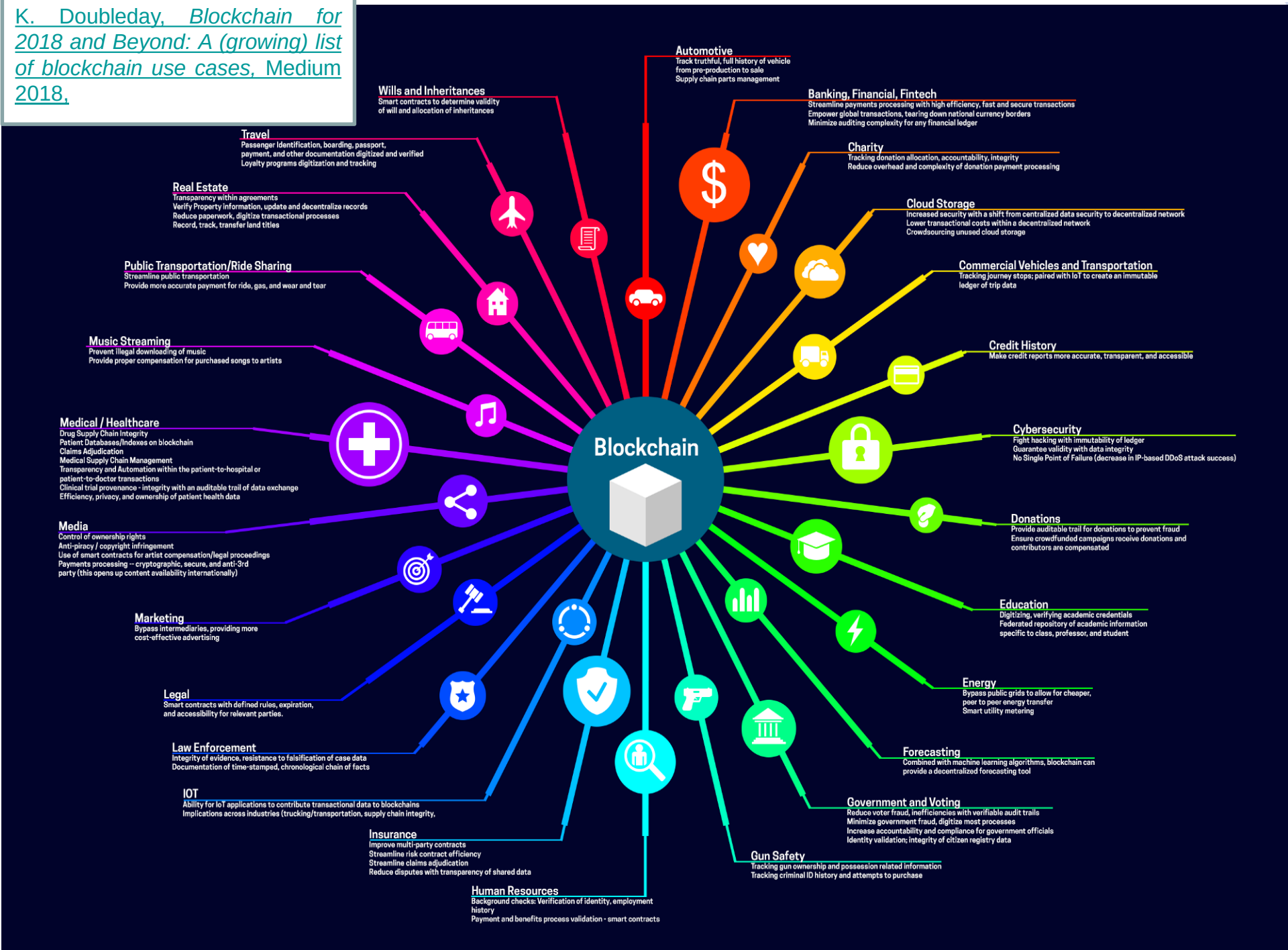
Dane osobowe a usługi FinTech

Blockchain

- Personal data and/in the blockchain
- Data protection and the blockch
  - Close
  - Open

More questions than answers!

K. Doubleday, *Blockchain for 2018 and Beyond: A (growing) list of blockchain use cases*, Medium 2018,



Dane osobowe a usługi FinTech

Blockchain

- **Every/Any Industry**
  - Information-sharing across organizations - trust, transparency, and efficiency
  - Supply Chain Management - With FlureeDB, a consortium of stakeholders in a supply chain can own, operate and enforce rules for their own shared blockchain.
  - Coordinate logistics, payments, financial terms, and contract rules
  - End-to-End visibility and tracking of supply chain process in real-time
  - Auditing - Records can be instantly independently verified.
  - Compliance - Track processes against regulations with pre-defined rules
  - Business Contracts -- Set pre-defined rules for transactions between two or more companies engaged in a partnership
- **Automotive**
  - Track truthful, full history of vehicle from pre-production to sale
  - Supply chain parts management
- **Banking, Financial, Fintech**
  - Streamline payments processing with high efficiency, fast and secure transactions
  - Empower global transactions, tearing down national currency borders
  - Minimize auditing complexity for any financial ledger
- **Charity**
  - Tracking donation allocation, accountability, integrity
  - Reduce overhead and complexity of donation payment processing

- **Cloud Storage**
  - Increased security with a shift from centralized data security to decentralized network
  - Lower transactional costs within a decentralized network
  - Crowdsourcing unused cloud storage
- **Commercial Vehicles and Transportation**
  - Tracking journey stops; paired with IoT to create an immutable ledger of trip data
- **Credit History**
  - Make credit reports more accurate, transparent, and accessible
- **Cybersecurity**
  - Fight hacking with immutability of ledger
  - Guarantee validity with data integrity
  - No Single Point of Failure (decrease in IP-based DDoS attack success)
- **Donations**
  - Provide auditable trail for donations to prevent fraud
  - Ensure crowdfunded campaigns receive donations and contributors are compensated
- **Education**
  - Digitizing, verifying academic credentials
  - Federated repository of academic information specific to class, professor, and student
- **Energy**
  - Bypass public grids to allow for cheaper, peer to peer energy transfer
  - Smart utility metering
- **Forecasting**
  - Combined with machine learning algorithms, blockchain can provide a decentralized forecasting tool

- **Government and Voting**
  - Reduce voter fraud, inefficiencies with verifiable audit trails
  - Minimize government fraud, digitize most processes
  - Increase accountability and compliance for government officials
  - Identity validation; integrity of citizen registry data
- **Gun Safety**
  - Tracking gun ownership and possession related information
  - Tracking criminal ID history and attempts to purchase
- **Human Resources**
  - Background checks: Verification of identity, employment history
  - Payment and benefits process validation - smart contracts
- **Insurance**
  - Improve multi-party contracts
  - Streamline risk contract efficiency
  - Streamline claims adjudication
  - Reduce disputes with transparency of shared data
- **Internet of Things**
  - Ability for IoT applications to contribute transactional data to blockchains
  - Implications across industries (trucking/transportation, supply chain integrity, etc.)
- **Law enforcement**
  - Integrity of evidence, resistance to falsification of case data
  - Documentation of time-stamped, chronological chain of facts
- **Legal**
  - Smart contracts with defined rules, expiration, and accessibility for relevant parties.

- **Marketing**
  - Bypass intermediaries, providing more cost-effective advertising
- **Media**
  - Control of ownership rights
  - Anti-piracy / copyright infringement
  - Use of smart contracts for artist compensation/legal proceedings
  - Payments processing -- cryptographic, secure, and anti-3rd party (this opens up content availability internationally)
- **Medical / Healthcare**
  - Drug Supply Chain Integrity
  - Patient Databases/Indexes on blockchain
  - Claims Adjudication
  - Medical Supply Chain Management
  - Transparency and Automation within the patient-to-hospital or patient-to-doctor transactions
  - Clinical trial provenance - integrity with an auditable trail of data exchange
  - Efficiency, privacy, and ownership of patient health data
- **Public Transportation/Ride Sharing**
  - Streamline public transportation
  - Provide more accurate payment for ride, gas, and wear and tear
- **Real Estate**
  - Transparency within agreements
  - Verify property information, update and decentralize records
  - Reduce paperwork, digitize transactional processes
  - Record, track, transfer land titles
- **Travel**
  - Passenger Identification, boarding, passport, payment, and other documentation digitized and verified
  - Loyalty programs digitization and tracking
- **Wills and Inheritances**
  - Smart contracts to determine validity of will and allocation of inheritances

Dane osobowe a usługi FinTech

Blockchain

- By design

- Anonymous? (Bitcoin example)
  - obvious ‘identities’, name or pseudonym, not collected or used
  - online wallets or exchange services ➔ personal identity linked to bitcoin operations
  - every transaction is stored publicly and permanently
  - a bitcoin address per transaction? ➔ Big data!!!!

Dane osobowe a usługi FinTech

Closed Blockchain

- Permissioned private blockchains ➔ easy scenario (?)

- Most probably but data protection applies:
  - Lawfulness, purpose limitation...
  - Data subject rights!!!
    - Right to rectification, right to erasure, portability...
  - Data retention!

Dane osobowe a usługi FinTech

Open Blockchain

- Public, immutable, everlasting personal data...
- + *peer-to-peer* architecture ➔ Perfect (DP) storm.

- Issues:
  - Controllership, legal basis, purpose, data access rights...

- Let's reflect together, the DP and the 'blockchain community'

Dane osobowe a usługi FinTech

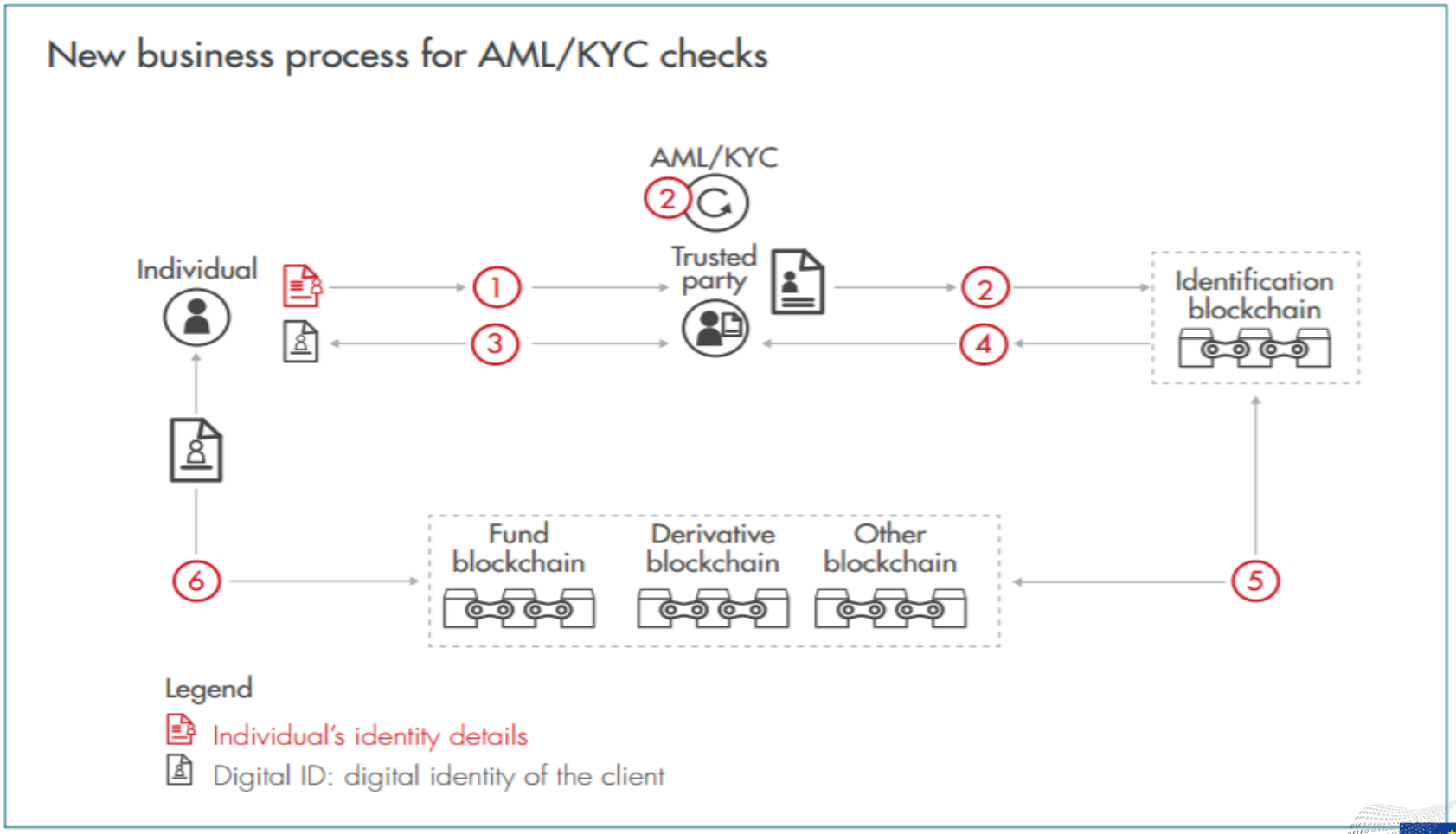
Blockchain

- Anonymity in public blockchain

- Privacy management in private blockchain
  - Hyperledger – Linux based project established in 2015 with the objective to advance cross-industry collaboration by developing blockchains and distributed ledgers, with a particular focus on improving the performance and reliability of these systems (as compared to comparable cryptocurrency designs) so that they are capable of supporting global business transactions by major technological, financial and supply chain companies.[5] The project will integrate independent open protocols and standards by means of a framework for use-specific modules, including blockchains with their own consensus and storage routines, as well as services for identity, access control and smart contracts.

Dane osobowe a usługi FinTech

Blockchain



Source: Deloitte: Out of the blocks Blockchain: from hype to prototype, May 2016

Dane osobowe a usługi FinTech

Some questions on personal data and blockchain

- *Applicability of rules on territorial Scope?*
- *Controllership*
- *Application of the household exemption*
- *Application of data protection principles*
- *No way to forget?*

Dane osobowe a usługi FinTech

Re-use of bitcoin-like services

Namecoin

expected to lead to:

- Identity systems,
- Messaging systems,
- Personal namespaces,
- Notary/timestamp systems, (!!!)
- Alias systems,
- Issuance of shares/stocks.

Crowdfunding

Crowdlending

Przykład - Passenger Name Record

Advance Passenger Information (API)

Podstawowa informacja, która w transporcie lotniczym identyfikuje pasażera lub członka załogi. Obejmuje **imię i nazwisko, datę urodzenia, płeć, obywatelstwo oraz identyfikator dokumentu podróżnego** (np. numer paszportu). Ten zakres informacyjny może być odczytany maszynowo z paszportu lub dowodu osobistego. Przewoźnicy gromadzą dane API, gdy rejestrują pasażera.

Passenger Name Record

Zapis w bazie danych zamieszczony w systemie rezerwacyjnym (CRS), który **zawiera dane pasażera, opis jego rezerwacji i podróży**. IATA i ATA zdefiniowały standardy PNR dla ruchu lotniczego, lecz nie istnieje jeden wspólny wykaz danych w PNR dla wszystkich CRS.

Choć PNR został stworzony dla transportu lotniczego, jest dziś wykorzystywany szeroko w innych sektorach transportu, przy rezerwacji hoteli i wypożyczaniu samochodów.

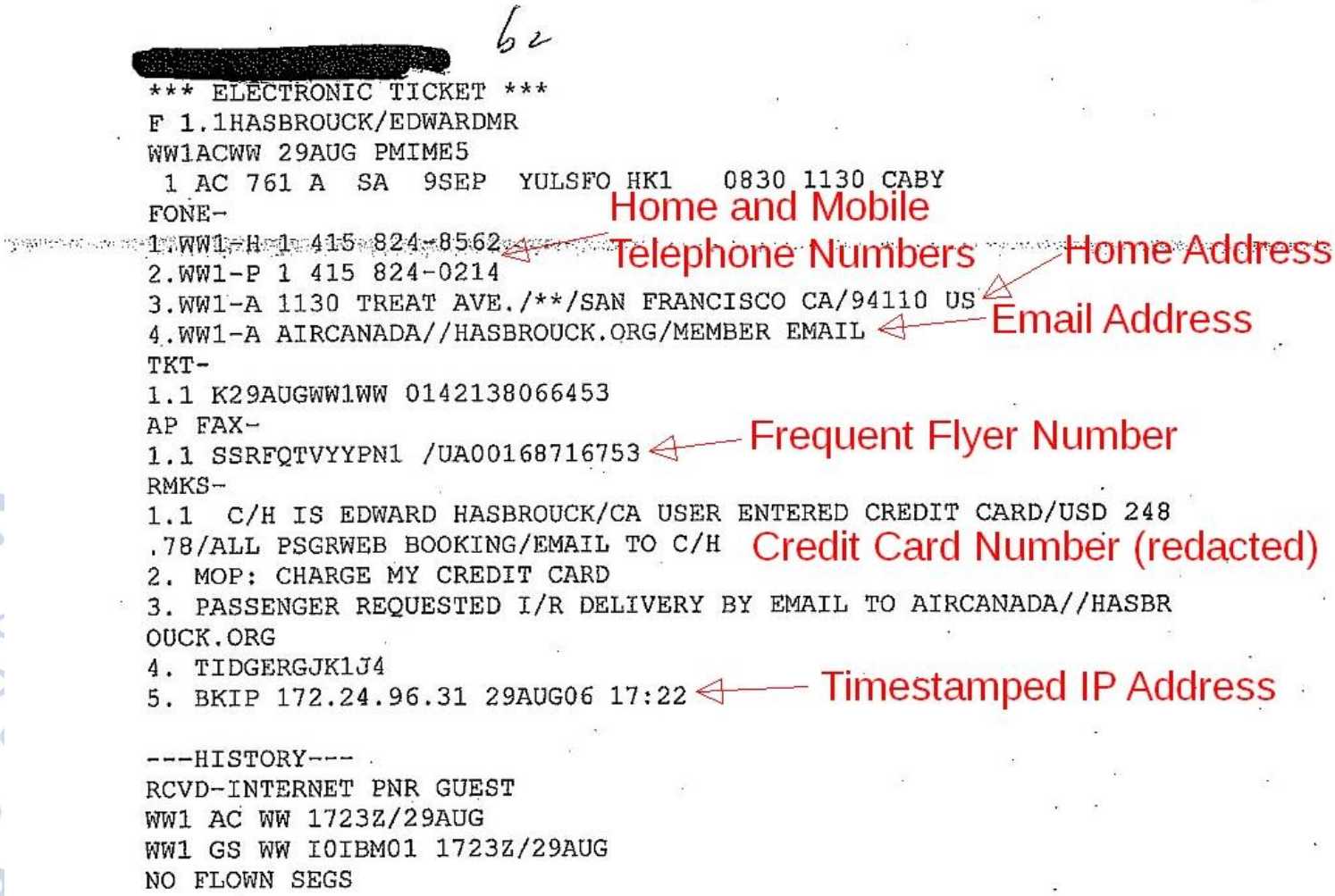
Czym jest Passenger Name Record

Zawartość standardowego PNR

- Identyfikacja pasażera,
- Identyfikacja travel agent lub biura podróży,
- Informacje o bilecie (numer biletu lub termin ważności biletu),
- Informacja o co najmniej jednym segmencie podróży,
- Identyfikacja osoby dostarczającej informacji lub dokonującej rezerwacji,

Inne informacje takie jak znak czasu, *pseudo-city code* agencji zapisywane są w CRS automatycznie.

Czym jest Passenger Name Record



Patrz: *Edward Hasbrouck*, PNR, The Practical Nomad, artykuł stale aktualizowany wersja z 5.4.2017 r. https://hasbrouck.org/articles/PNR.html

Czym jest Passenger Name Record

```
1.HASEROUCK/EDWARD MR(ADT)
2     AF   83      N 13JAN 2 SFOCDG B 1      I   1535 1125 1
3     AF   7183    L 14JAN 3 CDGZYR B 1      TN  1235 1412
4     AF   7186    L 20JAN 2 ZYRCDG HK1          1609 1746
5     AF   84      N 21JAN 3 CDGSFO HK1      2E  1015 1255
6    SEA   RQST AF HK1 CDGSFO /41AN  /P2/S4
7    SSR   cccc AF HK1     /P2/S4
8    AP  1-4158240214
9    AP  AF@HASBROUCK.ORG
```

This PNR from my ATS file with CBP includes the details of my travel by train between Paris and Brussels (ZYR). Of course the PNR also shows my seat assignment (41A from CDG to SFO), so relationships between passengers can be analyzed, even if they made reservations and bought tickets separately.

2 April 2013 Edward Hasbrouck, The Identity Project 21 of 34

Patrz: *Edward Hasbrouck*, Government Surveillance and Control of Travelers, The Cato Institute, Waszyngton, 2.4.2013 r. https://hasbrouck.org/articles/Hasbrouck-Cato-2APR2013.pdf

Czym jest Passenger Name Record

W praktyce na potrzeby PNR w CRS zapisuje się m.in.

- Dane o wykorzystanej taryfie (przynajmniej typ taryfy, ale również ograniczenia, które mogą dotyczyć biletu),
- Podatki opłacone,
- Forma płatności,
- Dodatkowe informacje kontaktowe agenta,
- Dodatkowe informacje kontaktowe pasażera,
- Cele podróży,
- Wiek pasażera (jeśli ma wpływ na zasady podróżowania lub opłaty),
- Dane o wykorzystywanych systemach lojalnościowych lub statusie stałego klienta,
- Miejsce przypisane pasażerowi (lub wskazania co do miejsca),
- Szczególne usługi (SSR) takie jak wymagania pokarmowe, wózki itp.
- Informacje o innych usługach lub usługach opcjonalnych (OSI) mogą one obejmować m.in. dane kontaktowe dodatkowych osób, powiązanie z osobą obsługującą pasażera, język używany, informacje o niepełnosprawności lub chorobach,
- Uwagi sprzedawcy (reakcja na poszczególne części zamówienia i limity czasowe)

Czym jest Passenger Name Record

Władze poszczególnych krajów dodatkowo wymagają zawarcia w PNR danych takich jak:

- płeć,
- dane paszportowe (obywatelstwo, identyfikatory, data ważności),
- data urodzenia,
- informacje na temat wizy wjazdowej (numer wizy, miasto, w którym została wydana, datę wydania, kraj na terytorium którego wiza jest ważna),
- informacje o zezwoleniu miejscowych władz na wjazd do regionów szczególnych,
- dane kart stałego pobytu (takich jak Zielona Karta)
- tzw. Redress Number pasażera
- miejsce urodzenia pasażera (miasto)
- adres zamieszkania pasażera w kraju docelowym,
- adres tymczasowego w kraju docelowym,
- adres pierwszego noclegu w kraju docelowym,
- wszelkie informacje o płatnościach i rachunkach.

Czym jest Passenger Name Record

W nowym systemie mają być przetwarzane dane wszystkich pasażerów podróżujących z lub do Unii Europejskiej. Profil osoby („rekord PNR”) trafi do specjalnej krajowej bazy danych.

Profil obejmuje:

- dane osobowe pasażera (imię, nazwisko, adres, numer dokumentu etc.);
- szczegółowe dane o samym locie (data, godzina, trasa, typ maszyny);
- dane osoby, która dokonała rezerwacji;
- formę płatności (łącznie z numerem wykorzystanej karty kredytowej);
- specjalne życzenia pasażera (w tym informacja o poruszaniu się na wózku lub o ciąży);
- numer miejsca w samolocie;
- numer biletu;
- numer przypisany w programie lojalnościowym;
- informacje o nadanym lub zabranym na pokład bagażu;
- adnotacje o niestawieniu się na lot, zmianie miejsca czy nietypowym lub irytującym zachowaniu pasażera (wprowadzane przez obsługę linii lotniczych).

Co zwalczamy ?

1. Udział w organizacji przestępczej
2. Handel ludźmi
3. Wykorzystywanie seksualne dzieci i pornografia dziecięca
4. Nielegalny handel narkotykami i substancjami psychotropowymi
5. Nielegalny handel bronią, amunicją i materiałami wybuchowymi
6. Korupcja
7. Oszustwo, w tym oszustwo przeciwko interesom finansowym Unii
8. Pranie dochodów z przestępstwa i fałszowanie pieniędzy, w tym euro
9. Przestępczość komputerowa i cyberprzestępczość
10. Przestępstwa przeciwko środowisku
11. Ułatwianie bezprawnego wjazdu i pobytu
12. Zabójstwo, spowodowanie ciężkiego uszczerbku na zdrowiu
13. Nielegalny obrót organami i tkankami ludzkimi
14. Uprowadzenie, bezprawne pozbawienie wolności i wzięcie zakładników
15. Kradzież zorganizowana i rozbój przy użyciu broni
16. Nielegalny handel dobrami kultury, w tym antykami i dziełami sztuki
17. Podrabianie i piractwo produktów
18. Fałszowanie dokumentów urzędowych i handel nimi
19. Nielegalny handel substancjami hormonalnymi i innymi śr. pobudzającymi wzrost
20. Nielegalny handel materiałami jądrowymi lub promieniotwórczymi
21. Zgwałcenie
22. Przestępstwa podlegające jurysdykcji Międzynarodowego Trybunału Karnego
23. Bezprawne zawładnięcie statkiem powietrznym lub statkiem
24. Sabotaż
25. Handel skradzionymi pojazdami
26. Szpiegostwo przemysłowe.

Co można wyczytać z twojego biletu lub karty pokładowej ?

Title: MR First Name: JOHN Last Name: BRAVO
PNR: QR5172
From: LHR To: JFK Flight No: AA51
Date (YYYY-MM-DD): 2016-04-08
Class: Business Seat: 12A Seq No: 15
OK

M1BRAVO/JOHNMR EQR5172 LHRJFKAA 0051 099C012A0015 100

Patrz: Marcin Maj, *Jak za darmo wejść do biznesowego saloniku na lotnisku?* Niebezpiecznik.pl, 9.8.2016 r.

https://niebezpiecznik.pl/post/hackowanie-kart-pokladowych/

Co można wyczytać z twojego biletu lub karty pokładowej ?

	New item number	Element Description	Field Size	Unique / repeated	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Mandatory Items	1	Format Code	1	U	M																			
	5	Number of Legs Encoded	1	U	2																			
	11	Passenger Name	20	U	D	E	S	M	A	R	A	I	S	/	L	U	C							
	253	Electronic Ticket Indicator	1	U	E																			
	7	Operating carrier PNR Code	7	R	A	B	C	1	2	3														
	26	From City Airport Code	3	R	Y	U	L																	
	38	To City Airport Code	3	R	F	R	A																	
	42	Operating carrier Designator	3	R	A	C																		
	43	Flight Number	5	R	0	8	3	4																
	46	Date of Flight (Julian Date)	3	R	2	2	6																	
	71	Compartment Code	1	R	F																			
	104	Seat Number	4	R	0	0	1	A																
	107	Check-in Sequence Number	5	R	0	0	2	5																
	113	Passenger Status	1	R	1																			
	6	Field Size of variable size field (Conditional + Airline item 4)	2	R	4	D																		

- Patrz: Marcin Maj, *Jak za darmo wejść do biznesowego saloniku na lotnisku?* Niebezpiecznik.pl, 9.8.2016 r. https://niebezpiecznik.pl/post/hackowanie-kart-pokladowych/

Jak zhakować systemy rezerwacji biletów znając podstawowe dane z PNR ?

TECHSPOT

LOGIN

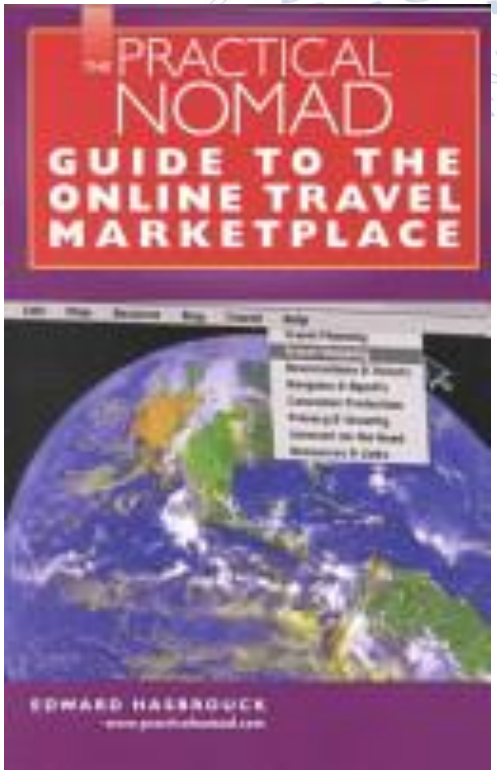
TRENDING REVIEWS FEATURES BEST OF DOWNLOADS PRODUCT FINDER FORUMS

systems will be fixed soon, although others might require a deeper changes in how the system works.

PNRs can be gathered offline

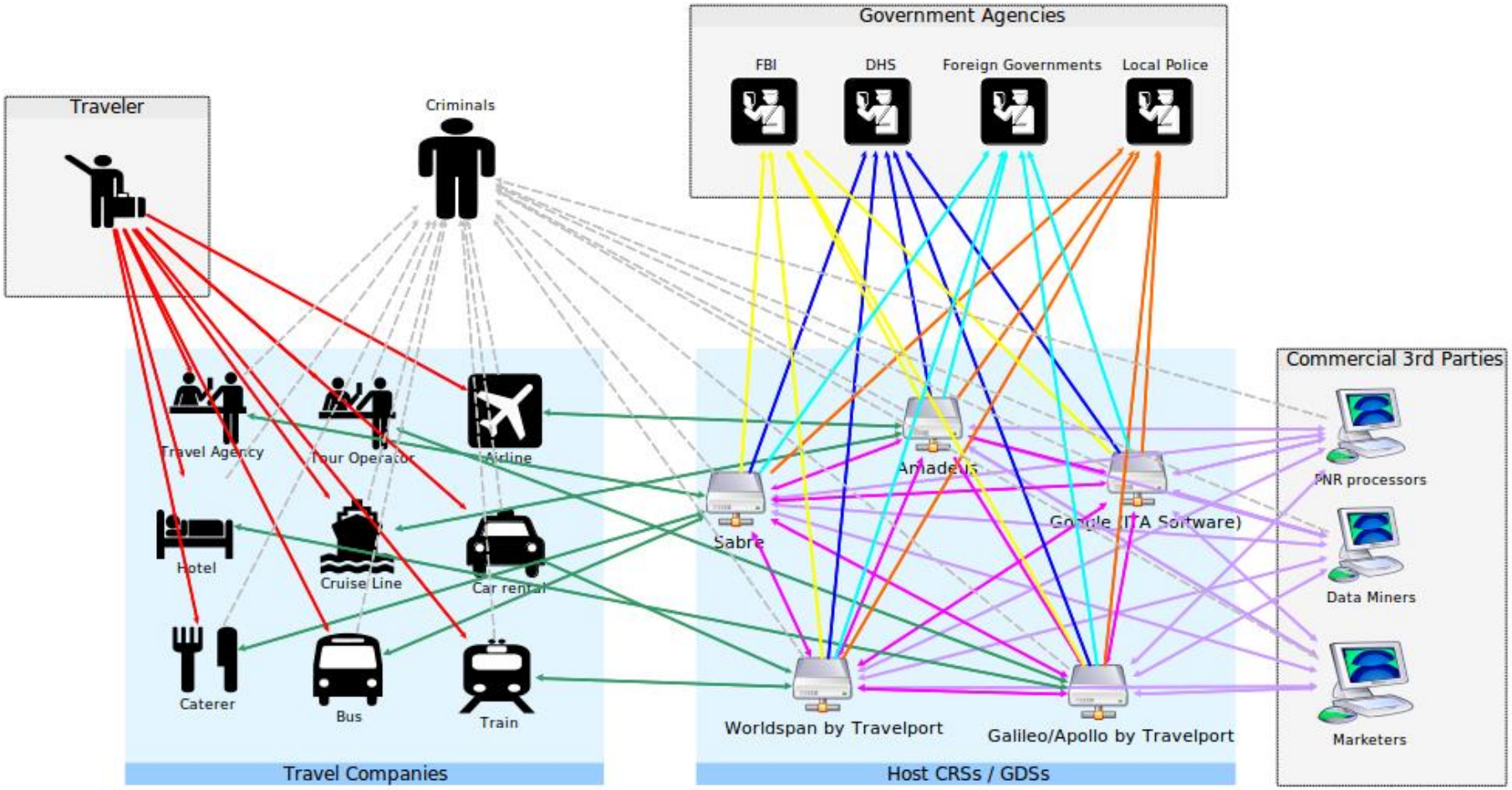
- *Jose Vilches*, Flight reservations can be easily hacked with a last name and PNR locator, Techspot 3.1.2017 r. *http://www.techspot.com/news/67625-flight-reservations-can-easily-hacked-last-name-pnr.html*

Jak zhakować systemy rezerwacji biletów znając podstawowe dane z PNR ?



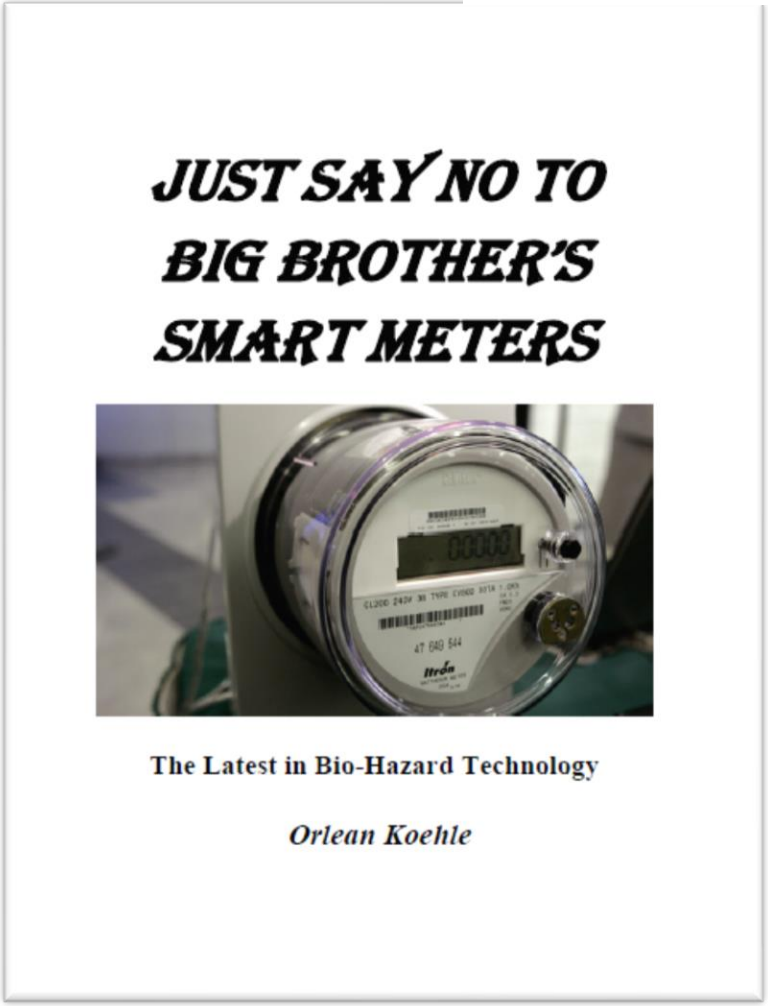
Patrz: *Edward Hasbrouck*, PNR, The Practical Nomad, artykuł stale aktualizowany wersja z 5.4.2017 r. https://hasbrouck.org/articles/PNR.html

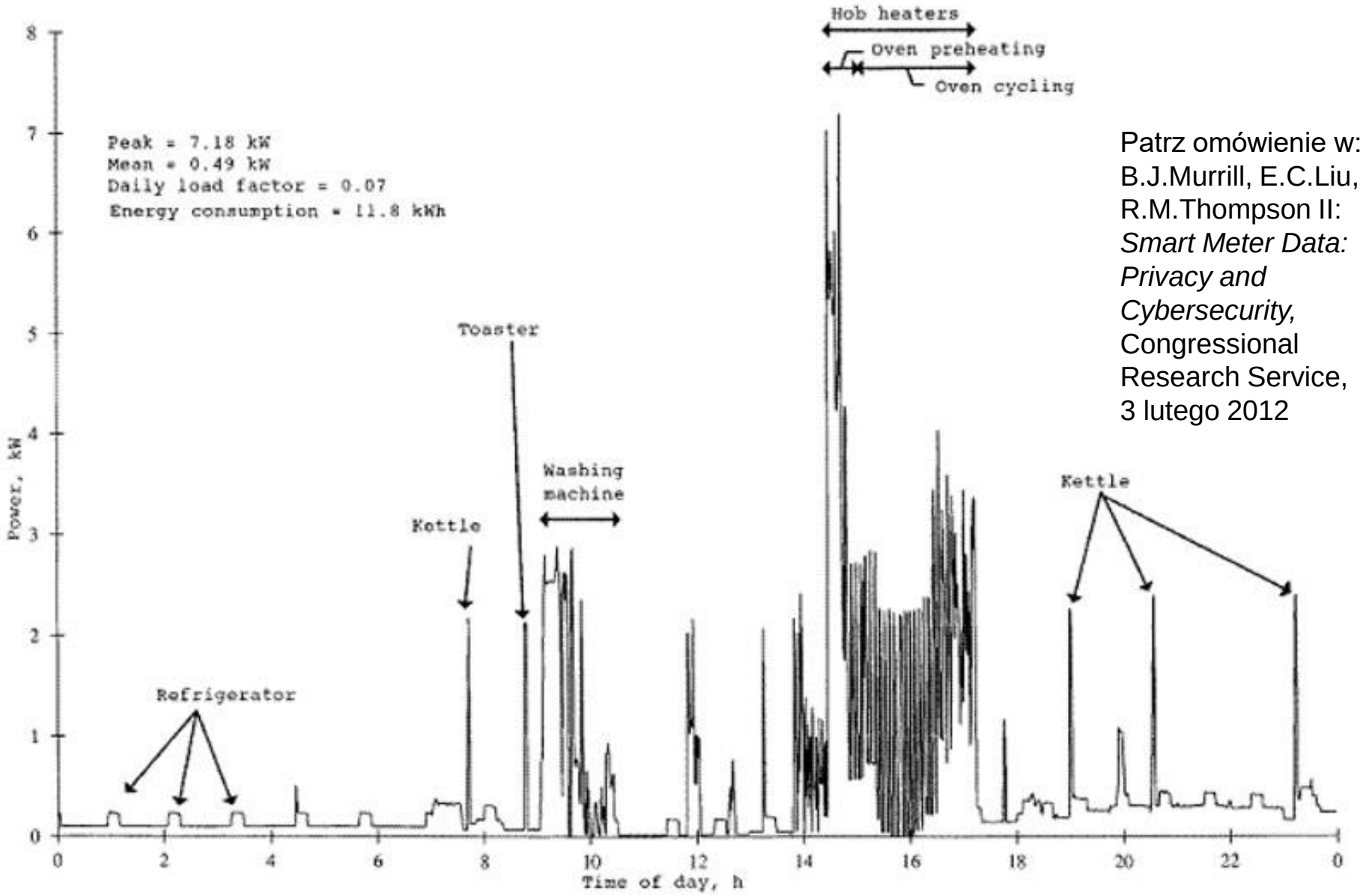
Jak zhakować systemy rezerwacji biletów znając podstawowe dane z PNR ?



Patrz: *Edward Hasbrouck*, PNR, The Practical Nomad, artykuł stale aktualizowany wersja z 5.4.2017 r. https://hasbrouck.org/articles/PNR.html

INTELIGENTNE LICZNIKI ENEGRETYCZNE
Smart metering / Smart grids





Patrz omówienie w:
B.J.Murrill, E.C.Liu, R.M.Thompson II: *Smart Meter Data: Privacy and Cybersecurity,* Congressional Research Service, 3 lutego 2012

INTELIGENTNE LICZNIKI ENEGRETYCZNE
Smart metering / Smart grids

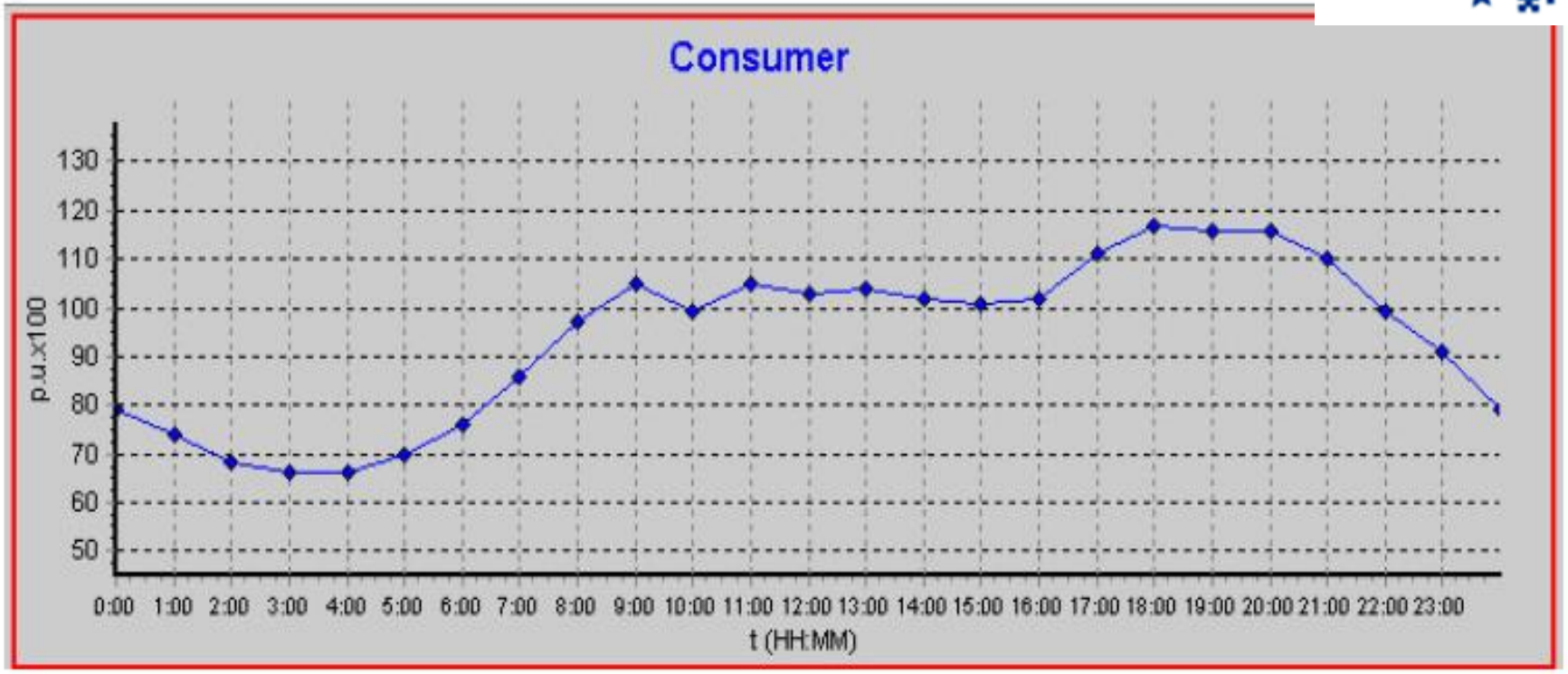


Figure 5 – Example Daily Consumer Load Profile

Operationalizing Privacy by Design:The Ontario Smart Grid Case Study, Information & Privacy Commissioner, Ontario, Toronto , luty 2011, str. 13.

Inteligentne miasto oparte o IoT

Inteligentne miasto XXI w.
- nie jest jednolitą strukturą stworzoną przez jednego architekta czy urbanistę.
- nie jest zespołem systemów zarządzanych centralnie przez centrum koordynacyjne na poziomie miasta, aglomeracji czy konurbacji

Jest zespołem z zasady otwartych systemów informacyjnych, które umożliwiają dynamiczne dołączanie do architektury inteligentnego miasta nowych komponentów.

Część z systemów pozostaje zamknięta i dostępna jedynie dla głównych twórców danego kompleksu *Smart City*, lecz z założenia należy przyjmować, że i te systemy dążyć będą w najbliższej przyszłości do większej otwartości.

Wszystkie systemy inteligentnego miasta, by przejawiać rzeczywistą „inteligencję" muszą stale reagować na zmieniające się otoczenie.

W naturalny sposób uznajemy, że nowoczesne inteligentne miast musi z zasady opierać się na infrastrukturze Internetu rzeczy.

Tzw. „prawo do bycia zapomnianym” w rozporządzeniu UE (RODO)

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.

Tzw. „prawo do bycia zapomnianym” w rozporządzeniu UE (RODO)

2. Jeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

3. Ust. 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;

b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3;

d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub

e) do ustalenia, dochodzenia lub obrony roszczeń.

Prawo do przenoszenia danych w rozporządzeniu UE (RODO)

1. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:
    a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz
    b) przetwarzanie odbywa się w sposób zautomatyzowany.
2. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.
3. Wykonanie prawa, o którym mowa w ust. 1 niniejszego artykułu, pozostaje bez uszczerbku dla art. 17. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.
4. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.

Ograniczenia ochrony danych w rozporządzeniu UE (RODO)

1. Prawo Unii lub prawo państwa członkowskiego, […] może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:

a) bezpieczeństwu narodowemu;
b) obronie;
c) bezpieczeństwu publicznemu;
d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;
e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu;
f) ochronie niezależności sądów i postępowania sądowego;
g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu;
h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej [a) – e) oraz g)];
i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób;
j) egzekucji roszczeń cywilnoprawnych.

Standardowe klauzule umowne

- Zarówno **w prawie RE**, jak i **w prawie UE** jest mowa o klauzulach umownych między administratorem dokonującym przekazania danych i odbiorcą w państwie trzecim jako możliwym sposobie zapewnienia wystarczającego stopnia ochrony danych u odbiorcy.
- Na **szczeblu UE** Komisja Europejska z pomocą Grupy Roboczej Art. 29 wypracowała standardowe klauzule umowne, które zostały oficjalnie uznane decyzją Komisji za dowód prawidłowej ochrony danych. Jako że decyzje Komisji są w całości wiążące w państwach członkowskich, organy krajowe odpowiedzialne za nadzorowanie transgranicznego przepływu danych muszą uwzględnić te standardowe klauzule umowne w swoich procedurach. Tak więc jeżeli administrator dokonujący przekazania danych oraz odbiorca z państwa trzeciego uzgodnią i podpiszą takie klauzule, powinny one wystarczyć organowi nadzorczemu za dowód, że wdrożono prawidłowe zabezpieczenia.
- Istnienie standardowych klauzul umownych w ramach prawnych UE nie uniemożliwia administratorom sformułowania innych doraźnych klauzul umownych. Muszą one jednak skutkować takim samym stopniem ochrony, jak zapewniany przez standardowe klauzule umowne. Najważniejszymi cechami standardowych klauzul umownych są:
- klauzula beneficjenta będącego stroną trzecią, która umożliwia osobom, których dane dotyczą, wykonywanie praw na podstawie umowy, mimo że nie są jej stroną;
- zgoda odbiorcy lub podmiotu odbierającego dane na poddanie się procedurom krajowego organu nadzorczego administratora przekazującego dane lub tamtejszych sądów w przypadku sporu.

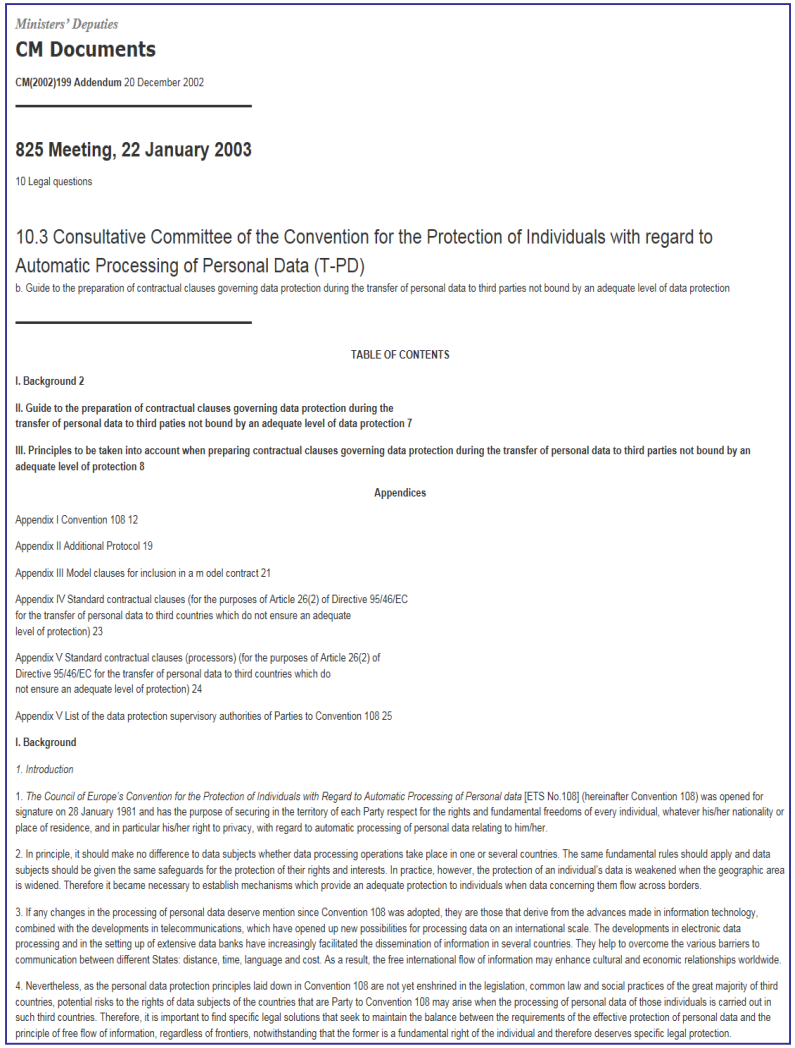
Standardowe klauzule umowne

- Dostępne są obecnie dwa zestawy standardowych klauzul w przypadku przekazywania danych **między administratorami**, spośród których administrator przekazujący dane może dokonać wyboru.
  - Zestaw I - Decyzja Komisji 2001/497/WE z dnia 15 czerwca 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, na mocy dyrektywy 95/46/WE, Dz.U. L 181 z 4.7.2001;
  - Zestaw II - Decyzja Komisji 2004/915/WE z dnia 27 grudnia 2004 r. zmieniająca decyzję 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, Dz.U. L 385 z 29.12.2004.

- W przypadku przekazywania danych przez administratora podmiotowi **przetwarzającemu** dostępny jest tylko jeden zestaw standardowych klauzul umownych.
  - Komisja Europejska (2010), Decyzja Komisji 2010/87 z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, Dz.U. L 39 z 12.2.2010.

Standardowe klauzule umowne

- W kontekście **prawa RE** Komitet Konsultacyjny Konwencji nr 108 opracował wskazówki dotyczące sporządzania klauzul umownych:



Ministers' Deputies

CM Documents

CM(2002)199 Addendum 20 December 2002

825 Meeting, 22 January 2003

10 Legal questions

10.3 Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD)

b. Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data protection

TABLE OF CONTENTS

I. Background

1. Introduction

1. *The Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal data* [ETS No.108] (hereinafter Convention 108) was opened for signature on 28 January 1981 and has the purpose of securing in the territory of each Party respect for the rights and fundamental freedoms of every individual, whatever his/her nationality or place of residence, and in particular his/her right to privacy, with regard to automatic processing of personal data relating to him/her.

2. In principle, it should make no difference to data subjects whether data processing operations take place in one or several countries. The same fundamental rules should apply and data subjects should be given the same safeguards for the protection of their rights and interests. In practice, however, the protection of an individual's data is weakened when the geographic area is widened. Therefore it became necessary to establish mechanisms which provide an adequate protection to individuals when data concerning them flow across borders.

3. If any changes in the processing of personal data deserve mention since Convention 108 was adopted, they are those that derive from the advances made in information technology, combined with the developments in telecommunications, which have opened up new possibilities for processing data on an international scale. The developments in electronic data processing and in the setting up of extensive data banks have increasingly facilitated the dissemination of information in several countries. They help to overcome the various barriers to communication between different States: distance, time, language and cost. As a result, the free international flow of information may enhance cultural and economic relationships worldwide.

4. Nevertheless, as the personal data protection principles laid down in Convention 108 are not yet enshrined in the legislation, common law and social practices of the great majority of third countries, potential risks to the rights of data subjects of the countries that are Party to Convention 108 may arise when the processing of personal data of those individuals is carried out in such third countries. Therefore, it is important to find specific legal solutions that seek to maintain the balance between the requirements of the effective protection of personal data and the principle of free flow of information, regardless of frontiers, notwithstanding that the former is a fundamental right of the individual and therefore deserves specific legal protection.

„Wskazówki co do sporządzania klauzul umownych dotyczących ochrony danych podczas przekazywania danych osobowych stronom trzecim niezapewniającym prawidłowego stopnia ochrony danych”

EDPS

STANDARD CONTRACTUAL CLAUSES OR BINDING CORPORATE RULES

STANDARD CONTRACTUAL CLAUSES

WHAT IS IT?
Contract between two legal entities.

PURPOSE
It allows the transfer of personal data from EEA to third countries not recognised as offering adequate protection.

LICENCE
Not required. Transfers based on the SCC may be made without requiring further authorization from the DPA.

LIABILITY
Enables data subjects to exercise contractual rights even though they are not a party to the contract; and, the recipient agrees to be subject to EU DPA and courts.

PROS
a)provided by the CoE. Ready to be used; b)can be added to main agreements; c)good for a particular data flow; d)best solution for small companies.

CONS
In cases of large companies to put in place, hundreds of model clauses will result in high administrative cost: file, storage, review and keep up to date.

BINDING CORPORATE RULES

WHAT IS IT?
Compulsory code of conduct within a group of companies or group of enterprises engaged in the same economic activity.

PURPOSE
It allows the transfer of personal data from EEA to third countries not recognised as offering adequate protection.

LICENCE
Required. But only by the lead DPA. No additional authorisations are required, and a uniform approval mechanism is set by GDPR.

LIABILITY
The BCR must be legally binding. The companies based in the EU are liable for breaches committed by any member not located in the EU.

PROS
Tailor Made. Allow large number of data flows for various purposes. Dealing with one DPA. No contract for each transfer. Plenty of EU guidelines. Good PR.

CONS
The final validation can take one year or more. Big expense; however, the cost is less than other ways of handling transfers. No valid for transfer to third parties.

www.lawinfographic.com

Wiążące reguły korporacyjne (BCR)

Wiążące reguły korporacyjne (BCR)

- Wielostronne wiążące reguły korporacyjne (BCR) bardzo często dotyczą jednocześnie kilku europejskich organów ochrony danych. Aby BCR mogły zostać zatwierdzone, ich projekt należy przesłać wraz ze standardowymi formularzami wniosków do organu wiodącego. Organ wiodący można zidentyfikować na podstawie standardowego formularza wniosku. Informuje on następnie wszystkie organy nadzorcze w państwach członkowskich EOG, w których działalność prowadzą podmioty stowarzyszone grupy, chociaż ich udział w procesie oceny BCR jest dobrowolny. Chociaż ocena ta nie ma charakteru wiążącego, wszystkie zainteresowane organy ochrony danych powinny uwzględnić jej wyniki w swoich formalnych procedurach udzielania zezwoleń.

Wiążące reguły korporacyjne (BCR)

- Treść i strukturę odpowiednich wiążących reguł korporacyjnych wyjaśniono w dokumentach Grupy Roboczej Art. 29:
  - *Working document setting up a framework for the structure of Binding Corporate Rules*
    [„Dokument roboczy ustanawiający **ramy struktury wiążących reguł korporacyjnych**”],
    WP 154, Bruksela, 24 czerwca 2008 r.;
  - *Working document setting up a table with the elements and principles to be found in Binding Corporate Rules*
    [„Dokument roboczy ustanawiający **tabelę zawierającą elementy i zasady, które powinny zostać uwzględnione w wiążących regułach korporacyjnych**”],
    WP 153, Bruksela, 24 czerwca 2008 r.
  - *Recommendation 1/2007 on the standard application for approval of binding corporate rules for the transfer of personal data* [„Rekomendacja nr 1/2007 w sprawie **standardowego wniosku o zatwierdzenie wiążących reguł korporacyjnych** w odniesieniu do przekazywania danych osobowych”],
    WP 133, Bruksela, 10 stycznia 2007 r.

Wiążące reguły korporacyjne (BCR) – GDPR (2016/679)

Artykuł 47 **wiążące reguły korporacyjnych** *(!!! Błąd w Dz.U. UE !!!)*

1. Właściwy organ nadzorczy zatwierdza wiążące reguły korporacyjne […], pod warunkiem że:

   a) są one prawnie wiążące oraz mają zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą, w tym ich pracowników, i są przez każdego z tych członków egzekwowane;

   b) wyraźnie przyznają osobom, których dane dotyczą, egzekwowalne prawa w związku z przetwarzaniem ich danych osobowych; oraz […]

2. W wiążących regułach korporacyjnych […], określone zostają co najmniej:

   a) struktura i dane kontaktowe odnośnej grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą i każdego z jej członków;

   b) jednorazowe lub wielokrotne przekazanie danych, w tym kategorie danych osobowych, rodzaj przetwarzania i jego cele, rodzaje osób, których dane dotyczą, oraz nazwa danego państwa trzeciego lub danych państw trzecich;

   c) ich prawnie wiążący charakter, wewnętrzny i zewnętrzny;

   d) zastosowanie ogólnych zasad ochrony danych – w szczególności ograniczenia celu, minimalizacji danych, ograniczonych okresów przechowywania, jakości danych, uwzględnianie ochrony danych w fazie projektowania oraz domyślnej ochrony danych, podstawa prawna przetwarzania, przetwarzanie szczególnych kategorii danych osobowych, środki zapewniające bezpieczeństwo danych, wymogi w zakresie dalszego przekazywania podmiotom niezwiązanym wiążącymi regułami korporacyjnymi;

Wiążące reguły korporacyjne (BCR) – GDPR (2016/679)

Artykuł 47 **wiążące reguły korporacyjnych** *(!!! Błąd w Dz.U. UE !!!)*

e) prawa osób, których dane dotyczą, w związku z przetwarzaniem oraz sposoby wykonywania tych praw, w tym z prawa do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu – w tym profilowaniu – […], prawa do wnoszenia skarg do właściwego organu nadzorczego i właściwych sądów państw członkowskich zgodnie z art. 79 oraz prawa do środka zaskarżenia, a w stosownych przypadkach – odszkodowania za naruszenie wiążących reguł korporacyjnych;

f) przyjęcie przez administratora lub podmiot przetwarzający posiadających jednostki organizacyjnej na terytorium państwa członkowskiego odpowiedzialności prawnej za naruszenie wiążących reguł korporacyjnych przez odnośnego członka niemającego jednostki organizacyjne w Unii; administrator lub podmiot przetwarzający są zwolnieni z tej odpowiedzialności – w całości lub w części – wyłącznie, gdy udowodni, że członek ten nie ponosi odpowiedzialności za wydarzenie, które doprowadziło do powstania szkody;

g) sposób, w jaki osobom, których dane dotyczą, podaje się […] informacje o wiążących regułach korporacyjnych, w szczególności o postanowieniach, o których mowa w lit. d), e) i f) niniejszego ustępu;

h)zadania inspektora ochrony danych […] lub innej osoby lub podmiotu odpowiedzialnych za monitorowanie przestrzegania wiążących reguł korporacyjnych w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz monitorowanie szkoleń i rozpatrywanie skarg;

i) procedury dotyczące skarg;

Wiążące reguły korporacyjne (BCR) – GDPR (2016/679)

Artykuł 47 **wiążące reguły korporacyjnych** *(!!! Błąd w Dz.U. UE !!!)*

j) stosowane w grupie przedsiębiorstw lub w grupie przedsiębiorców prowadzących wspólną działalność gospodarczą mechanizmy zapewniające weryfikację przestrzegania wiążących reguł korporacyjnych. Mechanizmy takie obejmują audyty w zakresie ochrony danych oraz metody zapewniania działań naprawczych mających chronić prawa osób, których dane dotyczą. Wyniki takiej weryfikacji powinny być przekazywane osobie lub podmiotowi, o których mowa w lit. h), oraz zarządowi przedsiębiorstwa sprawującego kontrolę w grupie przedsiębiorstw lub organowi kierującemu grupą przedsiębiorców prowadzących wspólną działalność gospodarczą i powinny być dostępne na żądanie właściwego organu nadzorczego;

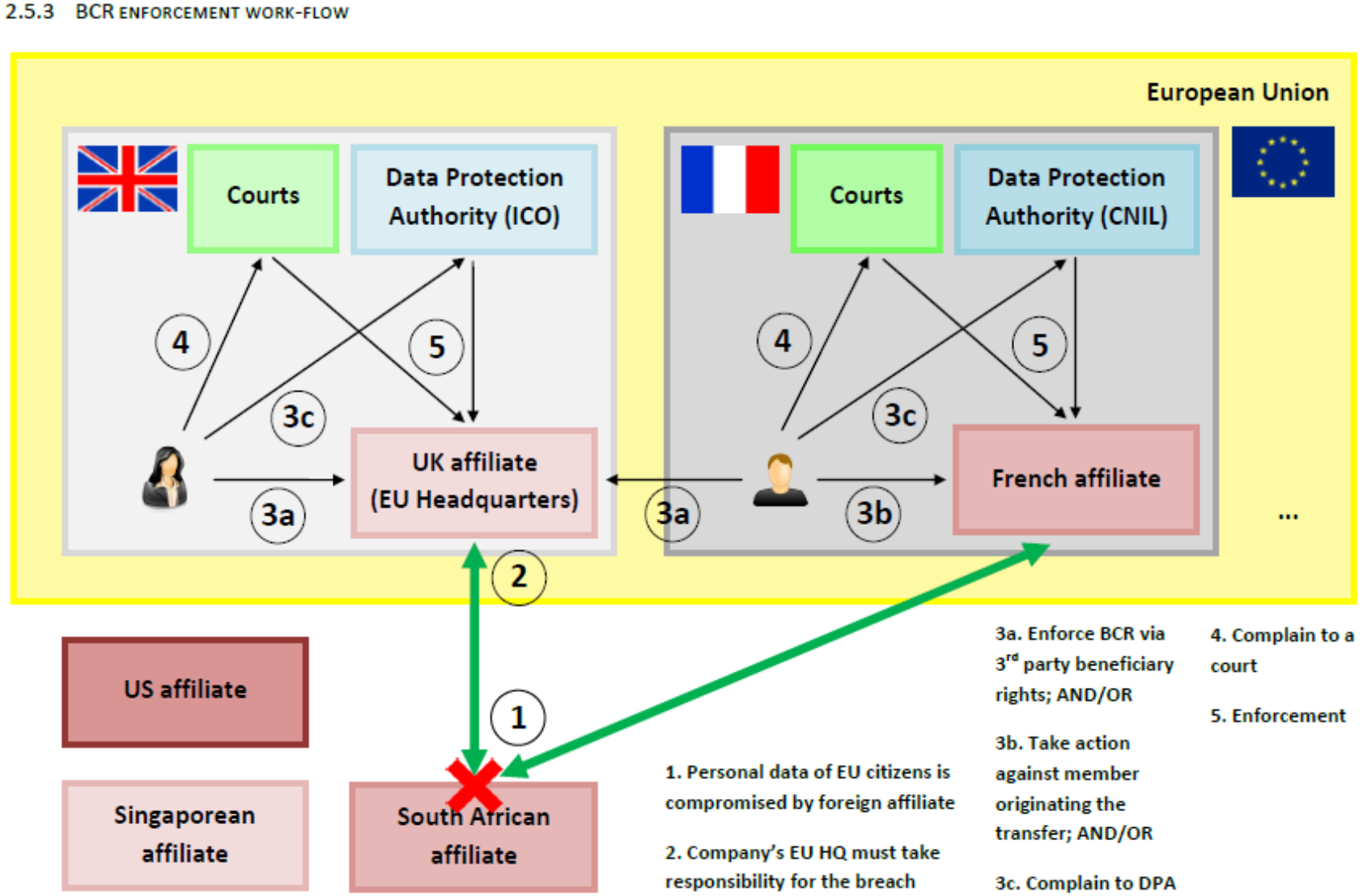
k) mechanizmy zgłaszania i rejestrowania zmian w zasadach i zgłaszania tych zmian organowi nadzorczemu;

l) mechanizm współpracy z organem nadzorczym zapewniający przestrzeganie zasad przez wszystkich członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą, w szczególności poprzez udostępnianie organowi nadzorczemu wyników weryfikacji środków, o której mowa w lit. j);

m) mechanizm zgłaszania właściwemu organowi nadzorczemu wszelkich wymogów prawnych, którym podlega w państwie trzecim członek grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą i które mogą mieć istotny niekorzystny wpływ na gwarancje przewidziane w wiążących regułach korporacyjnych; oraz

n) właściwe szkolenia z zakresu ochrony danych dla personelu mającego stały lub regularny dostęp do danych osobowych. […]

Wiążące reguły korporacyjne (BCR) – GDPR (2016/679)



109 *Framework for Personal Information Transfers: Comparison and Assessment of EU BCR and APEC CBPR Systems,* Information Integrity Solutions, wrzesień 2013, s. 14, https://informationintegritysolutions.squarespace.com/s/IIS-CBPR-BCR-report-FINAL.pdf

Zatwierdzone BCR

Company name	Lead authority
ABN AMRO Bank N.V.	Dutch DPA
Astra Zeneca plc	ICO (UK)
Accenture	ICO (UK)
Airbus (Controller)	CNIL (FR)
Akastor ASA (Controller)	Norwegian DPA
Aker Solutions ASA (Controller)	Norwegian DPA
Akzo Nobel N.V. (Controller)	Dutch DPA
Align Technologies B.V. (Controller and Processor)	Dutch DPA
American Express	ICO (UK)
ArcelorMittal Group	Luxemburg
Atmel	ICO (UK)
Atos (Controller and Processor)	CNIL (FR)
AXA	CNIL (FR)
Axa Private Equity	CNIL (FR)
BakerCorp International Holdings Inc. (Controller)	Dutch DPA
BMC Software (Controller and Processor)	CNIL (FR)
BMW	DPA of Bavaria (Germany)
BP	ICO (UK)
Bristol Myers Squibb	CNIL (FR)
CA plc	ICO (UK)
Capgemini (Controller and Processor)	CNIL (FR)
Cardinal Health, Inc.	IDPC (MT)
Care Fusion	ICO (UK)
Cargill, Inc.	ICO (UK)
Citigroup	ICO (UK)
CMA-CGM	CNIL (FR)
Continental Group	DPA of Lower Saxony (Germany)
Corning (Controller)	CNIL (FR)
D.E. Master Blenders 1753 ("DEMB") ex Sara Lee International B.V. (indirect subsidiary of Sara Lee Corporation)	Dutch DPA
Deutsche Post DHL	BfDI, Germany
Deutsche Telekom	BfDI, Germany
DSM	Dutch DPA
e-Bay	Luxemburg
ENGIE (ex GDF SUEZ; Controller)	CNIL (FR)
Ernst & Young	ICO (UK)
First Data Corporation (Controller and Processor)	ICO (UK)
Fluor Corporation Inc.	ICO (UK)
Flextronics International Ltd	ICO (UK)
General Electric (GE)	CNIL (FR)
Giesecke & Devrient	DPA of Bavaria (Germany)
GlaxoSmithKline plc	ICO (UK)
Hermès	CNIL (FR)
HP Enterprise (Controller)	CNIL (FR)
HP Inc. (ex Hewlett Packard; Controller)	CNIL (FR)
Hyatt	ICO (UK)
IMS Health Incorporated	ICO (UK)
ING Bank N.V.	Dutch DPA
Intel Corporation	Ireland
International SOS	CNIL (FR)
Johnson Controls	Belgian DPA
JPMC	ICO (UK)
Koninklijke DSM N.V. and affiliated companies	Dutch DPA
Kvaerner ASA	Norwegian DPA
LeasePlan Corporation N.V. (Controller)	Dutch DPA
Legrand (Controller)	CNIL (FR)
Linkbynet (Controller and Processor)	CNIL (FR)
Linklaters	ICO (UK)
LVMH	CNIL (FR)
Maersk Group	Danish DPA
Mastercard (Controller and Processor)	Belgian DPA
Merck Sharp & Dohme (MSD)	Belgian DPA
Michelin	CNIL (FR)
Motorola Mobility LLC	ICO (UK)
Motorola Solutions, Inc.	ICO (UK)
NetApp Inc. (Controller)	Dutch DPA
NOVARTIS	CNIL (FR)
Novo Nordisk A/S	Danish DPA
Nutreco N.V.(Controller)	Dutch DPA
Osram	DPA of Bavaria (Germany)
OVH	CNIL (FR)
Rabobank Nederland	Dutch DPA
Rockwool	Danish DPA
Royal Philips Electronics	Dutch DPA
Safran	CNIL (FR)
Salesforce (Processor)	CNIL (FR)
Sanofi Aventis	CNIL (FR)
Schlumberger Ltd.	Dutch DPA
Schneider Electric	CNIL (FR)
Shell International B.V.	Dutch DPA
Siemens Group	DPA of Bavaria (Germany)
Simon-Kucher & Partners	DPA of North Rhine-Westphalia (Germany)
Société Générale	CNIL (FR)
Sopra HR Software (ex HR Access; Controller and Processor)	CNIL (FR)
Spencer Stuart	ICO (UK)
Starwood Hotels and Resorts (Controller)	Belgian DPA
TMF Group B.V. (Controller and Processor)	Dutch DPA
Total	CNIL (FR)
UCB (Controller)	Belgian DPA

Stan na dzien 22.11.2017

EDPS

Tarcza prywatności (Privacy Shield) jako następstwo unieważnienia systemu Bezpiecznej Przystani (Safe Harbor)

Transfer danych – Dyrektywa 95/46

[Odpowiedni stopień ochrony – „adekwatność”]

1. Państwa Członkowskie zapewniają, aby przekazywanie do państwa trzeciego danych osobowych poddawanych przetwarzaniu lub przeznaczonych do przetwarzania po ich przekazaniu mogło nastąpić tylko wówczas gdy, niezależnie od zgodności z krajowymi przepisami przyjętymi na podstawie innych przepisów niniejszej dyrektywy, dane państwo trzecie zapewni **odpowiedni stopień ochrony**.
2. Odpowiedni stopień ochrony danych zapewnianej przez państwo trzecie należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zbioru takich operacji; szczególną uwagę zwracać się będzie na charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia, przepisy prawa, zarówno ogólne jak i branżowe, obowiązujące w państwie trzecim oraz przepisy zawodowe i środki bezpieczeństwa stosowane w tym państwie. (…)
6. **Komisja może stwierdzić** […], **że państwo trzecie zapewnia prawidłowy stopień ochrony** w znaczeniu ust. 2 niniejszego artykułu, co wynika z jego prawa krajowego lub międzynarodowych zobowiązań, jakie państwo to przyjęło, szczególnie po zakończeniu negocjacji […], w zakresie ochrony życia prywatnego i podstawowych praw i wolności osób fizycznych.

Państwa Członkowskie podejmują środki niezbędne w celu wykonania decyzji Komisji

Bezpieczna Przystań (Safe Harbor) 2000-2015

Rozwiązanie prawne dotyczące adekwatności ochrony danych przez niektóre podmioty w Stanach Zjednoczonych nie odnosi się w rzeczywistości do zbioru przepisów prawnych, lecz do przypominających kodeks postępowania zasad znanych pod nazwą **zasad ochrony prywatności w ramach „bezpiecznej przystani'** (ang. *Safe Harbor Privacy Principles*). UE i USA wspólnie wypracowały na początku XX w. te zasady w odniesieniu do amerykańskich przedsiębiorstw.

System utrzymał się do 2015 r., gdy został unieważniony przez TSUE w wyroku w sprawie *M.Schremsa*.

Przystąpienie do programu bezpiecznej przystani polegało na złożeniu Departamentowi Handlu USA dobrowolnego zobowiązania, które zostaje udokumentowane w wykazie publikowanym przez Departament. Jednym z ważnych elementów prawidłowości jest skuteczne wdrożenie ochrony danych, więc w zasadach bezpiecznej przystani przewidziano także pewien nadzór ze strony państwa: do systemu zasad przystąpić mogą tylko przedsiębiorstwa podlegające nadzorowi Federalnej Komisji Handlu USA.

Podręcznik europejskiego prawa o ochronie danych, Agencja Praw Podstawowych UE (FRA), Luksemburg 2014, Wyd. polskie, s. 143; http://giodo.gov.pl/259/id_art/7572/j/pl

Bezpieczna Przystań (Safe Harbor) 2000-2015

Decyzja KE w sprawie Safe Harbor 2000/520/WE z 26 lipca 2000 r.

Przyjęta przez Komisję na podstawie art. 25 ust. 6 dyrektywy 95/46.
Adekwatny poziom ochrony przekazywania danych ze Wspólnot do Stanów Zjednoczonych, uznany na podstawie decyzji, miał zostać osiągnięty, jeżeli organizacje będą przestrzegać zasad ochrony prywatności w ramach »bezpiecznej przystani« dotyczących ochrony danych osobowych przekazywanych z państwa członkowskiego do Stanów Zjednoczonych i najczęściej zadawanych pytań (FAQ), zawierających wytyczne dotyczące wprowadzania w życie zasad wydanych przez Rząd Stanów Zjednoczonych w dniu 21 lipca 2000 r. Ponadto organizacje miały publicznie ujawniać stosowane przez nie polityki ochrony prywatności, oraz powinny być poddane Federalnej Komisji Handlu (FTC)] na podstawie sekcji 5 ustawy o FTC, która zakazuje nieuczciwych lub wprowadzających w błąd czynów bądź praktyk handlowych lub wpływających na handel, bądź innego ustawowego organu
[…]
Dla zachowania przejrzystości i w celu zagwarantowania właściwym władzom w państwach członkowskich możliwości zapewnienia ochrony osób fizycznych w zakresie przetwarzania ich danych osobowych, konieczne jest wyszczególnienie w niniejszej decyzji okoliczności wyjątkowych, w których zawieszenie określonych przekazów danych powinno być usprawiedliwione, bez względu na to czy stwierdzono ich właściwą ochronę”.

Tarcza Prywatnosci (Privacy Shield)

- Orzeczeniem z 6 października 2015 r. w sprawie Schrems (C-362/14) Trybunał Sprawiedliwości UE unieważnił decyzję Komisji Europejskiej 2000/520/WE z 26 lipca 2000 r. w sprawie zapewniania przez podmioty z USA adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach "bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (notyfikowana jako dokument nr C(2000) 2441).
- Tym samym transfery danych pomiędzy Europą a USA stanęły pod znakiem zapytania, a administratorzy danych musieli szukać innych przesłanek legalizujących transfer, jednocześnie czekając na kolejne porozumienie w sprawie przekazywania danych między tymi kontynentami.
- Odpowiedź na problemy przyszła 12 lipca 2016 r., kiedy to Komisja Europejska przyjęła decyzję wdrażającą umowę Tarczy Prywatności, stwierdzając tym samym, że Stany Zjednoczone zapewniają odpowiedni poziom ochrony danych osobowych Europejczyków.

  - Decyzja KE w sprawie Safe Harbor 2000/520/WE z 26 lipca 2000 r.
  - Orzeczenie z 6 października 2015 r. w sprawie Schrems (C-362/14)
  - Decyzja wykonawcza KE w sprawie Tarczy Prywatnosci 2016/1250 z 12 lipca 2016 r.

Max Schrems
v. Facebook
czyli
gdzie diabeł nie może,
tam studenta pośle

Sprawy Maximilliana Schremsa

Max Schrems (ur. 1987)

Studiuje w Santa Clara

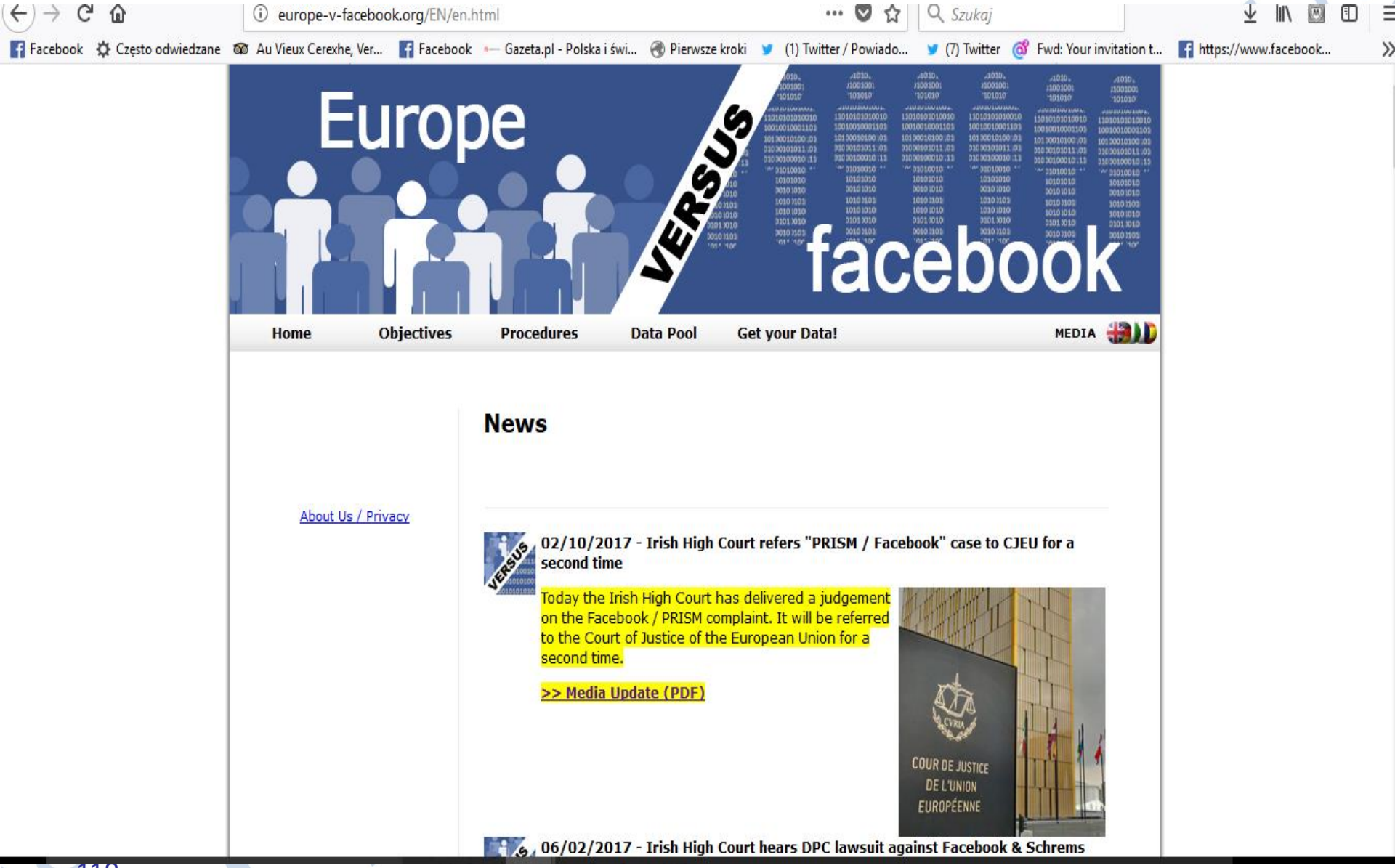
2011 – skargi do Irlandzkiego DPA

Historia skarg:
http://europe-v-facebook.org/EN/Complaints/complaints.html

23 skargi w latach 2011-2014

Ostatecznie 31 lipca 2014 r. M.Schrems wycofał wszystkie 22 pierwotne skargi (została tylko skarga w sprawie PRISM) uznając, że irlandzki DPA nie chce wydać decyzji, a jednocześnie uniemożliwia mu korzystanie z podstawowych praw strony sporu (dostęp do danych i dowodów zebranych w sprawie).

Sprawy Maximilliana Schremsa



Sprawy Maximilliana Schremsa

Skargi w sprawie “PRISM”

Po ujawnieniu rewelacji Edwarda Snowdena w czerwcu 2013 r. M.Schrems wniósł 5 skarg do organów ochrony danych w Irlandii, Luksemburgu i Niemczech przeciwko Facebook, Apple, Skype, Microsoft and Yahoo! uznając, że firmy bezprawnie przekazywały dane do amerykańskiego NSA w ramach projektu PRISM.

Ponieważ biura europejskiej tych podmiotów przekazywały dane do Stanów Zjednoczonych na podstawie porozumienia Bezpiecznej Przystani (Safe Harbor) w oparciu o decyzję 2000/520 Komisji Europejskiej, sprawa PRISM wkrótce przerodziła się w sprawę o znaczenie pojęcia adekwatności.

Chyba jednak sam M. Scherms nie spodziewał się, że pytanie w jego sprawie skierowane do TSUE przez sąd doprowadzi do unieważnienia całej decyzji i usunięcia z porządku prawnego Unii porozumienia *Safe Harbor*

Sprawy Maximilliana Schremsa

Sprawa w Irlandii zakończyła się orzeczeniem w 2015 r.

Sprawa w Luksemburgu trwa.

Sprawa w Niemczech zanikła gdzieś pomiędzy Bawarią a federalnym niemieckim organem ochrony danych.

Sprawa PRISM

Sprawa standardowych klauzul umownych

Pozew zbiorowy w Austrii

M.Schrems zakłada stowarzyszenie o nazwie NOYB (Not Of Your Business, którego zadaniem będzie prowadzenie sporów sądowych w sprawach ochrony danych osobowych i ochrony prywatności

M.Schrems opowiada o historii swych swoich sporów podczas panelu w trakcie 26. Dorocznej Konferencji nt. Komunikacji i Konkurencji (*26th IBA Annual Communications and Competition Conference*) zorganizowanej przez Międzynarodowe Stowarzyszenie Prawników (*International Bar Association*) w Londynie w dniach 11-12 maja 2015 r. https://vimeo.com/131638383 od 29'20"

Sprawy Maximilliana Schremsa

Odpowiedni poziom - adekwatność

Ani art. 25 ust. 2 dyrektywy 95/46, ani żaden inny jej przepis nie zawierają definicji pojęcia „odpowiedniego stopnia ochrony”.

„73 Oczywiście termin „odpowiedni” zawarty w art. 25 ust. 6 dyrektywy 95/46 oznacza, że od państwa trzeciego nie można wymagać zapewnienia poziomu ochrony identycznego z tym, jaki jest zagwarantowany w unijnym porządku prawnym. Tym niemniej[…], wyrażenie „odpowiedni stopień ochrony” należy rozumieć jako wymagające od tego państwa trzeciego skutecznego zapewnienia, ze względu na jego ustawodawstwo wewnętrzne lub zobowiązania międzynarodowe, poziomu ochrony podstawowych praw i wolności **merytorycznie równoważnego** poziomowi gwarantowanemu w Unii na mocy dyrektywy 95/46 w związku z kartą. W braku takiego wymogu cel wymieniony w poprzedzającym punkcie niniejszego wyroku zostałby bowiem zaprzepaszczony. Ponadto wysoki poziom ochrony gwarantowany w dyrektywie 95/46 w związku z kartą można byłoby łatwo obejść poprzez przekazanie danych osobowych z Unii do państw trzecich w celu ich przetwarzania w tych państwach.

74 […] Jakkolwiek środki, z jakich to państwo trzecie korzysta w tym względzie dla zapewnienia takiego stopnia ochrony, mogą różnić się od środków wprowadzonych w Unii w celu zagwarantowania poszanowania wymogów płynących z tej dyrektywy w związku z kartą, to jednak środki te powinny w praktyce skutecznie zapewniać ochronę **merytorycznie równoważną** ochronie gwarantowanej w Unii.

75 W tych okolicznościach przy badaniu poziomu ochrony zapewnionego w państwie trzecim Komisja zobowiązana jest ocenić treść reguł mających zastosowanie w tym państwie wynikających z jego ustawodawstwa wewnętrznego lub ze zobowiązań międzynarodowych, a także praktykę zmierzającą do zapewnienia poszanowania tych reguł, przy czym instytucja ta powinna […] wziąć pod uwagę wszystkie okoliczności dotyczące przekazywania danych osobowych do państwa trzeciego

Sprawy Maximilliana Schremsa

Po unieważnieniu przez TSUE „Bezpiecznej Przystani” większość podmiotów – w tym Facebook – zaczęło korzystać ze standardowych klauzul umownych (SKU) jako podstawy do transferu danych do Stanów Zjednoczonych. Większość z nich traktowała to jako rozwiązanie tymczasowe do czasu zastąpienia unieważnionego programu nowym (ostatecznie uczyniono to w lipcu 2016 r. przy pomocy Tarczy Prywatności).

M.Schrems zakwestionował zastosowanie takiej podstawy prawnej, żądając zawieszenia możliwości przekazywania danych w oparciu o SKU (postępowanie przed irlandzkim organem ochrony danych).

M.Schrems uznaje, że decyzje o SKU zawierają te same błędy co Bezpieczna Przystań i powinny być unieważnione w oparciu o te same powody.

W 2017 r. Komisja zaktualizowała treść SKU.

Tarcza Prywatnosci (Privacy Shield)

- Orzeczeniem z 6 października 2015 r. w sprawie Schrems (C-362/14) Trybunał Sprawiedliwości UE unieważnił decyzję Komisji Europejskiej 2000/520/WE z 26 lipca 2000 r. w sprawie zapewniania przez podmioty z USA adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach "bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (notyfikowana jako dokument nr C(2000) 2441).
- Tym samym transfery danych pomiędzy Europą a USA stanęły pod znakiem zapytania, a administratorzy danych musieli szukać innych przesłanek legalizujących transfer, jednocześnie czekając na kolejne porozumienie w sprawie przekazywania danych między tymi kontynentami.
- Odpowiedź na problemy przyszła 12 lipca 2016 r., kiedy to Komisja Europejska przyjęła decyzję wdrażającą umowę Tarczy Prywatności, stwierdzając tym samym, że Stany Zjednoczone zapewniają odpowiedni poziom ochrony danych osobowych Europejczyków.

  - Decyzja KE w sprawie Safe Harbor 2000/520/WE z 26 lipca 2000 r.
  - Orzeczenie z 6 października 2015 r. w sprawie Schrems (C-362/14)
  - Decyzja wykonawcza KE w sprawie Tarczy Prywatnosci 2016/1250 z 12 lipca 2016 r.

TARCZA PRYWATNOŚCI UE-USA
FAQ DLA EUROPEJSKICH OSÓB FIZYCZNYCH[1]

W dniu 13 grudnia 2016 r. Grupa Robocza Art. 29 przyjęła dokument „Tarcza Prywatności UE-USA - Często zadawane pytania (FAQ) dla europejskich osób fizycznych" (WP 246).

Co to jest Tarcza Prywatności?

Tarcza Prywatności[2] jest mechanizmem samocertyfikowania dla przedsiębiorstw zlokalizowanych w Stanach Zjednoczonych. To ramy uznane przez Komisję Europejską za zapewniające odpowiedni poziom ochrony danych osobowych przekazywanych z podmiotu UE do przedsiębiorstwa z siedzibą w Stanach Zjednoczonych, a zatem jako element gwarancji prawnej dla takich operacji przekazywania danych.

Tarcza Prywatności UE-USA obowiązuje w pełni od 1 sierpnia 2016 r.

Tarcza Prywatności dotyczy wszelkich danych osobowych przekazywanych z podmiotu UE do USA, w tym danych handlowych, stanu zdrowia lub związanych z zasobami ludzkimi (danych HR), pod warunkiem że przedsiębiorstwo w USA będące odbiorcą dokonało samocertyfikacji zgodnie z ramami.

Jakie korzyści daje mi Tarcza Prywatności?

Tarcza Prywatności polega na zobowiązaniu amerykańskich przedsiębiorstw do przestrzegania zasad, reguł i obowiązków określonych w ramach Tarczy Prywatności.

Ramy te przyznają Ci pewną liczbę praw, w przypadku gdy Twoje dane osobowe były przekazane z podmiotu UE do Stanów Zjednoczonych. Przede wszystkim, masz prawo do otrzymania informacji o przekazaniu danych i prawo dostępu do danych, np. w celu sprostowania lub usunięcia Twoich danych osobowych, które zostały przekazane[3]. Możesz sprawdzić, czy przedsiębiorstwo z siedzibą w USA posiada certyfikat, sprawdzając wykaz podmiotów uczestniczących w programie Tarczy Prywatności dostępny pod adresem: www.privacyshield.gov.

Zachęcamy do kierowania ewentualnych zapytań dotyczących przetwarzania Twoich danych w pierwszej kolejności do przedsiębiorstwa amerykańskiego.

Jeśli problem nie został rozwiązany przez przedsiębiorstwo uczestniczące w programie Tarczy Prywatności lub istnieją przyczyny, dla których nie możesz kierować zapytania bezpośrednio, Twój krajowy organ ochrony danych będzie gotowy pomóc Ci w rozwiązaniu sprawy.

Jak mogę złożyć skargę?

Jeśli uważasz, że przedsiębiorstwo uczestniczące w programie Tarczy Prywatności UE-USA naruszyło swoje zobowiązania wynikające z Ram Tarczy Prywatności UE-USA lub naruszyło Twoje prawa wynikające z zasad Tarczy Prywatności, możesz złożyć skargę.

Jeśli chcesz złożyć skargę dotyczącą przedsiębiorstwa w USA certyfikowanego w Tarczy Prywatności, albo przedsiębiorstwa oświadczającego, że zostało certyfikowane, skorzystaj ze wspólnego formularza skargi, dostępnego tutaj (dostępny wkrótce) lub skontaktuj się z Twoim krajowym organem ochrony danych[4]. Przekaż Twojemu organowi ochrony danych jak najwięcej szczegółów dotyczących sprawy, co umożliwi organowi rozpatrzenie skargi w jak najlepszy sposób.

Powstanie nieformalna grupa organów ochrony danych UE w celu rozpatrywania skarg dotyczących danych osobowych związanych z zasobami ludzkimi przekazanych z podmiotu UE do przedsiębiorstwa certyfikowanego w Tarczy Prywatności UE-USA, w kontekście stosunku pracy lub gdy przedsiębiorstwo w USA będące odbiorcą dobrowolnie zgodziło się współpracować z europejskim organem ochrony danych.
Nieformalna grupa organów ochrony danych rozpocznie dochodzenie, podczas którego obie strony będą miały możliwość wyrażania swoich stanowisk. Jeśli jest to konieczne, w celu rozwiązania sprawy, nieformalna grupa może wydać "wskazówki", będące wiążącą decyzją dla przedsiębiorstwa uczestniczącego w Tarczy Prywatności w USA.

W przypadkach, w których nieformalna grupa organów ochrony danych nie jest organem właściwym, organy ochrony danych UE mają możliwość przekazania sprawy do organów USA (w szczególności, Federalna Komisja Handlu zobowiązała się do priorytetowego traktowania tak przekazanych spraw, a DoC ma wyraźny termin na rozpoznanie skarg). Zależnie od okoliczności sprawy, właściwy krajowy organ ochrony danych może również skorzystać z własnych uprawnień (np. zakaz albo zawieszenie przekazania danych) w stosunku do podmiotu eksportującego dane w UE.

Aby uzyskać więcej informacji o możliwości złożenia skargi, możesz skierować pytanie do krajowego organu ochrony danych. Organy ochrony danych opracowują obecnie wspólny formularz skargi, który będzie mógł być wykorzystywany przez osoby UE w celu złożenia skargi. Formularz skargi zostanie udostępniony możliwie jak najszybciej. Formularz skargi będzie opcjonalny, dlatego możesz już złożyć skargę, kontaktując się z krajowym organem ochrony danych.

*Proszę zwrócić uwagę, że wnioski dotyczące **dostępu przez amerykańskie organy publiczne do celów działalność agencji wywiadowczych** podlegają odmiennej procedurze. Skontaktuj się z krajowym organem ochrony danych w celu uzyskania dalszych informacji.*

[1] W tym kontekście osoby europejskie oznaczają każdą osobę fizyczną, niezależnie od jej obywtelstwa, której dane osobowe zostały przekazane przedsiębiorstwu amerykańskiemu zgodnie z Tarczą Prywatności UE-USA.
[2] Decyzja w sprawie adekwatności zasad ramowych Tarczy Prywatności EU-USA („Tarcza Prywatności") albo („Ramy") została przyjęta przez Komisję Europejską 12 lipca 2016 r. Została stworzona przez Komisję Europejską i Departament Handlu Stanów Zjednoczonych by zastąpić Decyzję w sprawie Bezpiecznej Przystani nr 2000//520/EC unieważnioną wyrokiem Trybunału Sprawiedliwości UE 6 sierpnia 2015 r.
[3] W celu uzyskania bardziej szczegółowych informacji dotyczących gwarancji dla przekazywanych danych i Twoich praw w ramach Tarczy Prywatności UE-USA zapoznaj się z Przewodnikiem dotyczącym Tarczy Prywatności UE-USA opublikowanym przez Komisję Europejską.
[4] Użyte zwroty" krajowy organ ochrony danych", "organ ochrony danych UE" lub "organ UE zajmujący się" odnoszą się również do EIOD, który będzie organem UE zajmującym się przypadkami, w których Twoje dane osobowe zostały przekazane przez instytucję UE do przedsiębiorstwa certyfikowanego w Tarczy Prywatności w USA.

Szczególne istrumenty prawa międzynarodowego publicznego

Transfer danych na podstawie umów międzynarodowych - PNR

Dane dotyczące przelotu pasażera

Dane dotyczące przelotu pasażera (dane PNR) są gromadzone przez przewoźników lotniczych podczas procesu rezerwacyjnego i obejmują nazwiska, adresy, dane kart kredytowych oraz numery miejsc pasażerów. Na mocy prawa USA linie lotnicze są zobowiązane udostępnić te dane Departamentowi Bezpieczeństwa Wewnętrznego przed odlotem pasażerów. Wymóg ten odnosi się do lotów do Stanów Zjednoczonych lub z ich terytorium.

Passenger Name Record jest zapisem w bazie danych stanowiącej część systemu rezerwacyjnego (CRS) prowadzonego przez przewoźnika, organizatora turystyki lub wyspecjalizowany podmiot trzeci, zawierający dane pasażera, opis jego rezerwacji i podróży. Nie istnieje jeden wspólny wykaz danych w PNR dla wszystkich CRS stosowanych w różnych sektorach transportu pasażerskiego, przy rezerwacji hoteli czy wypożyczaniu samochodów. Za wzór przyjmuje się standardy zdefiniowane dla ruchu lotniczego przez IATA i ATA. Choć PNR został stworzony dla transportu lotniczego, jest dziś wykorzystywany szeroko w innych sektorach transportu, przy rezerwacji hoteli i wypożyczaniu samochodów.

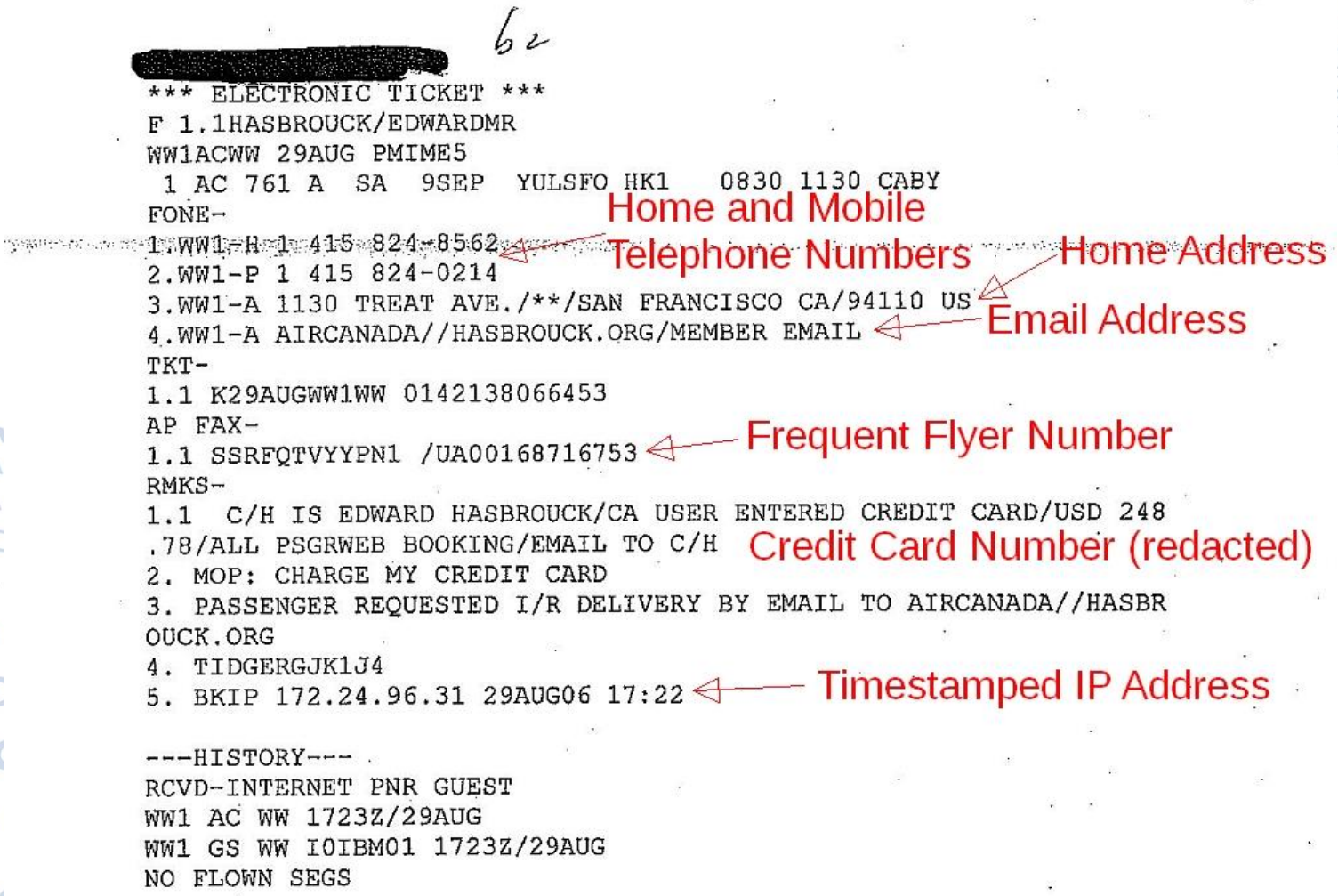
Transfer danych na podstawie umów międzynarodowych - PNR

Zawartość standardowego PNR

- Identyfikacja pasażera,
- Identyfikacja travel agent lub biura podróży,
- Informacje o bilecie (numer biletu lub termin ważności biletu),
- Informacja o co najmniej jednym segmencie podróży,
- Identyfikacja osoby dostarczającej informacji lub dokonującej rezerwacji,

Inne informacje takie jak znak czasu, *pseudo-city code* agencji zapisywane są w CRS automatycznie.

Transfer danych na podstawie umów międzynarodowych - PNR



Patrz: *Edward Hasbrouck*, PNR, The Practical Nomad, artykuł stale aktualizowany wersja z 5.4.2017 r. https://hasbrouck.org/articles/PNR.html

Transfer danych na podstawie umów międzynarodowych - PNR

Dane dotyczące przelotu pasażera

W celu zapewnienia prawidłowej ochrony danych PNR zgodnie z przepisami dyrektywy 95/46/WE, w 2004 r. przyjęto ‘pakiet PNR’ Pakiet ten dotyczył prawidłowości przetwarzania danych prowadzonego przez Departament Bezpieczeństwa Wewnętrznego USA (DHS).

- Decyzja Rady 2004/496/WE z 17 maja 2004 r. w sprawie zawarcia Porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych dotyczących przelotu pasażera (PNR) przez przewoźników lotniczych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, Biura Ceł i Ochrony Granic, Dz.U. L 183, str. 83,
- decyzja Komisji 2004/535/WE z 14 maja 2004 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Passenger Name Record (PNR) pasażerów lotniczych przekazywanych do Biura Ceł i Ochrony Granic Stanów Zjednoczonych, Dz.U. L 235, str. 11-22.

Transfer danych na podstawie umów międzynarodowych - PNR

Pakietu PNR został unieważniony przez TSUE w orzeczeniu w połączonych sprawach C-317/04 I C-318/04, *Parlament Europejski przeciwko Radzie Unii Europejskiej z* 30 maja 2006 r. pkt. 57, 58 i 59, w którym Trybunał orzekł jednocześnie, że zarówno decyzja o prawidłowości, jak i umowa dotycząca przetwarzania danych są wyłączone z zakresu dyrektywy.

W następstwie tego orzeczenia UE i Stany zjednoczone podpisały dwie odrębne umowy mające dwojaki cel: po pierwsze, mają stanowić podstawę prawną udostępnienia danych PNR organom USA, a po drugie, mają ustanowić prawidłową ochronę w kraju odbiorcy.

Pierwsza umowa podpisana w 2012 r. między krajami UE i Stanami Zjednoczonymi o sposobie udostępniania danych i zarządzania nimi została zastąpiona w tym samy roku inną umową w celu zapewnienia większej pewności prawnej. Nowa umowa została znacząco poprawiona. Ogranicza się w niej i wyjaśnia cele, dla których mogą być wykorzystywane informacje, takie jak zwalczanie poważnej przestępczości międzynarodowej i terroryzmu. W umowie określono okres przechowywania danych: po sześciu miesiącach dane należy zanonimizować. W przypadku niewłaściwego wykorzystania danych każdej osobie przysługuje prawo do administracyjnych i sądowych środków zaskarżenia zgodnie z prawem Stanów Zjednoczonych. Osoby mają też prawo dostępu do swoich danych PNR i ubiegania się o ich poprawienie przez Departament Bezpieczeństwa Wewnętrznego, w tym możliwość usunięcia danych, jeżeli informacje są niedokładne. Umowa, która weszła w życie dnia 1 lipca 2012 r., pozostanie w mocy przez siedem lat, do 2019 r.

Transfer danych na podstawie umów międzynarodowych - PNR

W grudniu 2011 r. Rada Unii Europejskiej zatwierdziła zawarcie zaktualizowanej umowy UE-Australia o przetwarzaniu i przekazywaniu danych PNR. Umowa między UE a Australią w sprawie danych PNR jest kolejnym krokiem realizacji programu UE, który obejmuje globalne wytyczne w sprawie danych PNR.

- Decyzja Rady 2012/381/UE z dnia 13 grudnia 2011 r. w sprawie zawarcia Umowy między Unią Europejską a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej i granicznej danych dotyczących przelotu pasażera (danych PNR), Dz.U. L 186 z 14.7.2012, s. 3. Tekst umowy, która zastąpiła poprzednią umowę z 2008 r., dołączono do decyzji, Dz.U. L 186 z 14.7.2012, s. 4–16.
- Komunikat Komisji z dnia 21 września 2010 r. w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim, COM(2010) 492 final, Bruksela, 21 września 2010 r. oraz *Opinia 7/2010 dotycząca komunikatu Komisji w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim*, WP 178, Bruksela, 12 listopada 2010 r

Transfer danych na podstawie umów międzynarodowych - PNR

- Parlament Europejski zwrócił się do TSUE o opinię na temat porozumienia Unii Europejskiej z Kanadą w sprawie wymiany danych dotyczących przelotów pasażerskich.
- Trybunał Sprawiedliwości
  - przyznał, że samo przekazywanie danych dotyczących przelotów – nawet dokonywane w sposób systematyczny – może co do zasady zostać uznane za dopuszczalne;
  - zgodził się z Parlamentem, że kilka spośród przepisów zawartych w projekcie porozumienia nie spełnia wymogów wynikających z prawa Unii;
  - zakwestionował systematyczne i ciągłe przekazywanie danych wszystkich pasażerów lotniczych kanadyjskiemu organowi, który miał mieć prawo do dalszego przekazywania ich innym organom kanadyjskim i zagranicznym w celu zwalczania terroryzmu i poważnej przestępczości międzynarodowej;
  - stwierdził, że umowa między UE a Kanadą powinna określić w bardziej jasny i precyzyjny sposób jakie dane mają być przekazywane oraz komu;
  - zażądał gwarancji, że nadzór nad przepisami dotyczącymi ochrony pasażerów linii lotniczych sprawować będzie się niezależny organ nadzorczy;
  - uznał, że planowana umowa pociąga za sobą ingerencji, które nie były ograniczone do tego, co jest absolutnie niezbędne i nie były zatem w pełni uzasadnione.

H.Hijmans PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators, European Data Protection Law Review nr 3, 2017, s. 310-312.

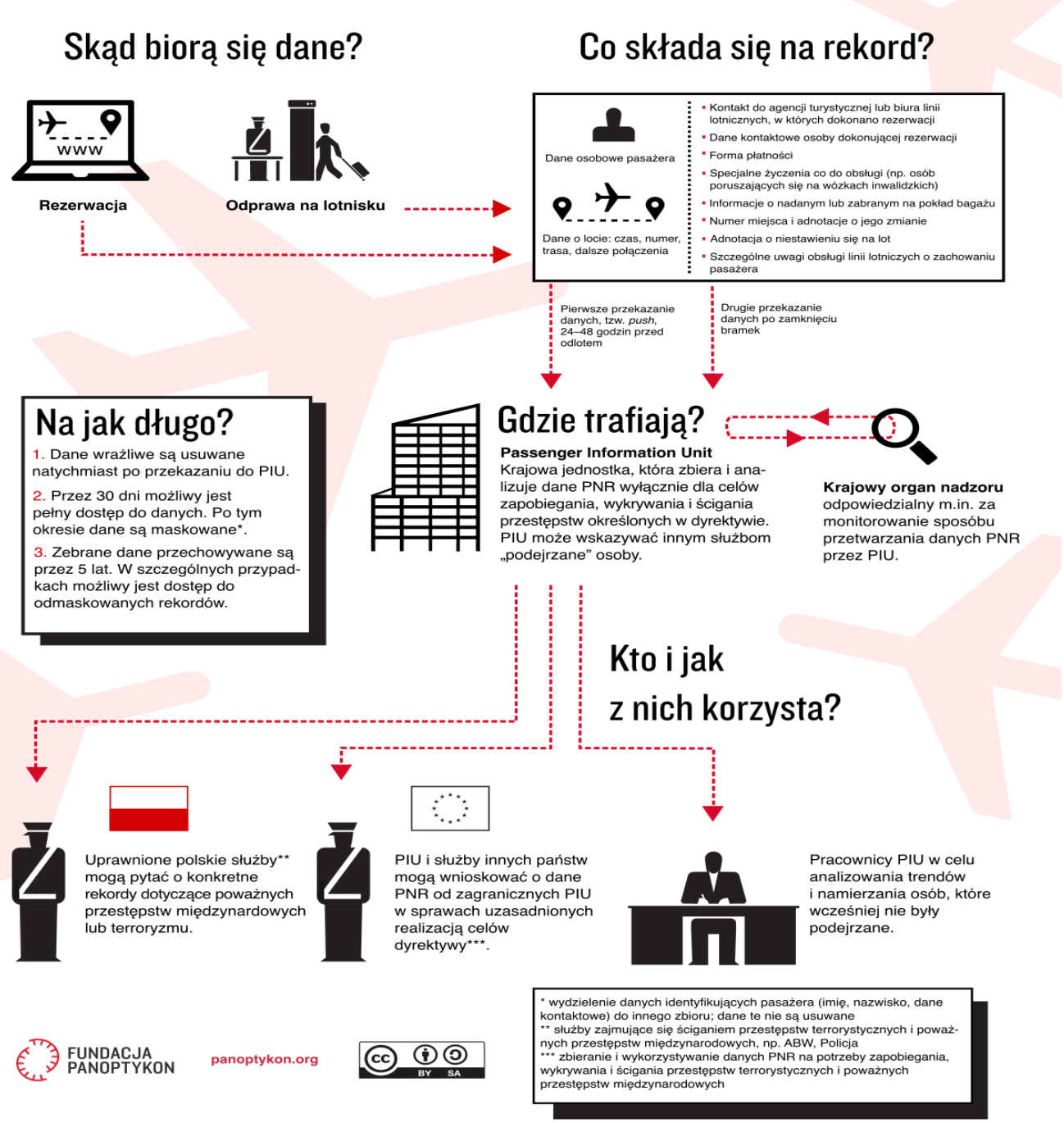
Regulacja unijna w sprawie PNR

- Dyrektywa Parlamentu Europejskiego i Rady (UE) **2016/681 (sic !!!)** z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, Dz.U. UE L 119, 4.5.2016, p. 132–149

  - (33) *Niniejsza dyrektywa nie wpływa na możliwość ustanowienia przez państwa członkowskie, na mocy przepisów krajowych, systemu zbierania i przetwarzania danych PNR przekazywanych przez podmioty gospodarcze niebędące przewoźnikami, takie jak biura podróży i organizatorzy wycieczek świadczący usługi związane z podróżowaniem, w tym rezerwację lotów, na potrzeby których zbierają i przetwarzają dane PNR, lub przez dostawców usług transportowych innych niż dostawcy określeni w niniejszej dyrektywie, pod warunkiem że takie przepisy krajowe są zgodne z prawem Unii.*

Co zwalczamy ?

1. Udział w organizacji przestępczej
2. Handel ludźmi
3. Wykorzystywanie seksualne dzieci i pornografia dziecięca
4. Nielegalny handel narkotykami i substancjami psychotropowymi
5. Nielegalny handel bronią, amunicją i materiałami wybuchowymi
6. Korupcja
7. Oszustwo, w tym oszustwo przeciwko interesom finansowym Unii
8. Pranie dochodów z przestępstwa i fałszowanie pieniędzy, w tym euro
9. Przestępczość komputerowa i cyberprzestępczość
10. Przestępstwa przeciwko środowisku
11. Ułatwianie bezprawnego wjazdu i pobytu
12. Zabójstwo, spowodowanie ciężkiego uszczerbku na zdrowiu
13. Nielegalny obrót organami i tkankami ludzkimi
14. Uprowadzenie, bezprawne pozbawienie wolności i wzięcie zakładników
15. Kradzież zorganizowana i rozbój przy użyciu broni
16. Nielegalny handel dobrami kultury, w tym antykami i dziełami sztuki
17. Podrabianie i piractwo produktów
18. Fałszowanie dokumentów urzędowych i handel nimi
19. Nielegalny handel substancjami hormonalnymi i innymi śr. pobudzającymi wzrost
20. Nielegalny handel materiałami jądrowymi lub promieniotwórczymi
21. Zgwałcenie
22. Przestępstwa podlegające jurysdykcji Międzynarodowego Trybunału Karnego
23. Bezprawne zawładnięcie statkiem powietrznym lub statkiem
24. Sabotaż
25. Handel skradzionymi pojazdami
26. Szpiegostwo przemysłowe.



Patrz:
Poznaj swój PNR: jakie dane z linii lotniczych trafią w ręce służb?
Fundacja Panoptykon, 13.07.2015

https://panoptykon.org/wiadomosc/poznaj-swoj-pnr-jakie-dane-z-linii-lotniczych-trafia-w-rece-sluzb

Przetwarzanie danych w „europejskim systemie PNR”

Zebrane dane dotyczące pasażerów linie lotnicze będą przekazywać do nowo utworzonych jednostek – tzw. *Passenger Information Units* (PIU). Państwom członkowskim pozostawiono decyzję o tym, jaki podmiot będzie realizował te zadania. Może to być nowy niezależny organ, ale zapewne w większości państw będzie on działał w ramach policji lub służb specjalnych. Dane będą przesyłane dwukrotnie. Pierwszy raz w przedziale 48–24 godzin przed odlotem oraz ponownie zaraz po zamknięciu bramek, kiedy lista pasażerów jest już ostateczna. PIU mają udostępniać dane innym uprawnionym organom na ich wyraźną i uzasadnioną prośbę. Również w tym przypadku decyzje o tym, które z organów publicznych mają być uprawnione do otrzymania takich danych pozostawiono Państwom Członkowskim. PIU mogą na podstawie nowych przepisów przeprowadzać własne analizy na podstawie zbieranych danych - np. na temat trendów w międzynarodowej przestępczości - i dzielić się wnioskami z odpowiednimi służbami.

Przez pierwsze 30 dni dane zebrane przez PIU będą przetwarzane i przekazywane innym organom (jeśli o to zawnioskują) w pełnym zakresie, ze wszystkimi szczegółami identyfikującymi pasażerów. Po upływie tego okresu dane będą oddzielane od danych bezpośrednio identyfikujących pasażera do oddzielnej bazy. Ponowne skojarzenie danych bezpośrednio identyfikujących pasażera z jego pełnym profilem będzie wymagało zgody szefa PIU. „Spseudonimizowane” profile PNR będą przetwarzane jeszcze przez 5 lat i gdy zajdzie taka potrzeba – przekazywane odpowiednim służbom. Najdłużej, bo aż przez cały ten okres, będzie można sięgnąć po PNR na potrzeby walki z terroryzmem.

„Poznaj swój PNR: jakie dane z linii lotniczych trafią w ręce służb?” Fundacja Panoptykon, 13.07.2015 https://panoptykon.org/wiadomosc/poznaj-swoj-pnr-jakie-dane-z-linii-lotniczych-trafia-w-rece-sluzb

Transfer danych na podstawie umów międzynarodowych – SWIFT / TFTP

Dane z komunikatów finansowych

Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (ang. *Society for Worldwide Interbank Financial Telecommunication*, SWIFT) z siedzibą w Belgii, które przetwarza większość globalnych przelewów środków z banków europejskich, prowadziło działania w bliźniaczym ośrodku w Stanach Zjednoczonych i Departament Skarbu USA zażądał od niego ujawnienia danych w związku z dochodzeniem dotyczącym terroryzmu.

- Grupa Robocza Art. 29, *Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing* [„Opinia 14/2001 w sprawie zagadnień ochrony danych związanych z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu”], WP 186, Bruksela, 13 czerwca 2011 r.;
- Grupa Robocza Art. 29, *Opinia 10/2006 w sprawie przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (Society for Worldwide Interbank Financial Telecommunication, SWIFT)*, WP 128, Bruksela, 22 listopada 2006 r.;
- Commission de la protection de la vie privée (belgijska komisja ds. ochrony prywatności) (2008), *Control and recommendation procedure initiated with respect to the company SWIFT scrl* [„Procedura kontroli i wydania rekomendacji zainicjowana w odniesieniu do spółki SWIFT scrl”], decyzja, 9 grudnia 2008 r.

Transfer danych na podstawie umów międzynarodowych – SWIFT / TFTP

Z punktu widzenia UE nie było wystarczających podstaw prawnych ujawnienia tych danych o charakterze zasadniczo europejskim, które były dostępne w Stanach Zjednoczonych wyłącznie dlatego, że znajdował się tam jeden z ośrodków przetwarzania danych SWIFT.

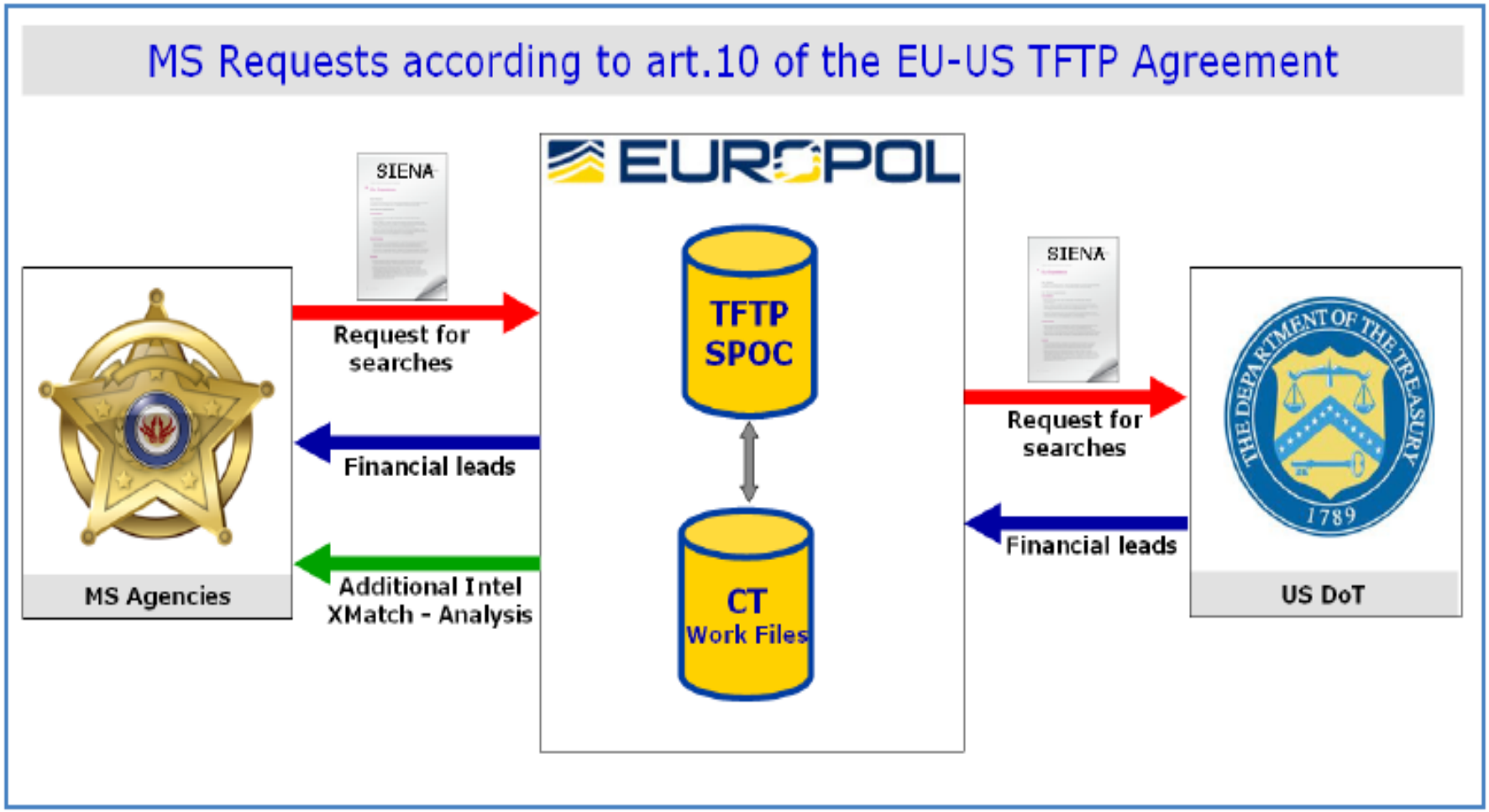
W 2010 r. zawarto specjalną umowę między UE a Stanami Zjednoczonymi, znaną jako umowa TFTP (niekiedy nazywana umową SWIFT), aby zapewnić niezbędną podstawę prawną i zapewnić prawidłowy stopień ochrony danych.

- Decyzja Rady 2010/412/UE z dnia 13 lipca 2010 r. w sprawie zawarcia Umowy między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu z Unii Europejskiej do Stanów Zjednoczonych danych z komunikatów finansowych do celów Programu śledzenia środków finansowych należących do terrorystów, Dz.U. L 195 z 27.7.2010, s. 3 i 4. Tekst umowy dołączono do decyzji, Dz.U. L 195 z 27.7.2010, s. 5–14.

Na mocy tej umowy dane finansowe przechowywane przez SWIFT są nadal udostępniane Departamentowi Skarbu USA w celu zapobiegania terroryzmowi, prowadzenia dochodzeń w sprawie terroryzmu, wykrywania bądź ścigania terroryzmu lub jego finansowania. Departament Skarbu USA może zwrócić się o dane finansowe SWIFT pod warunkiem, że wniosek:

- identyfikuje dane finansowe w możliwie jasny sposób;
- wyraźnie uzasadnia konieczność udostępnienia danych;
- posiada zakres określony w możliwie wąski sposób, aby zminimalizować ilość wnioskowanych danych;
- nie odnosi się do żadnych danych dotyczących jednolitego obszaru płatności w Euro (SEPA).

Transfer danych na podstawie umów międzynarodowych – SWIFT / TFTP



Transfer danych na podstawie umów międzynarodowych – SWIFT / TFTP

Europol otrzymuje kopię każdego wniosku skierowanego przez Departament Skarbu USA i weryfikuje, czy zasady umowy TFTP są przestrzegane. Jeżeli zostanie potwierdzone, że są one przestrzegane, SWIFT ma obowiązek dostarczyć dane finansowe bezpośrednio Departamentowi Skarbu USA. Departament ma obowiązek zabezpieczyć dane finansowe środkami ochrony fizycznej i udostępnić je wyłącznie analitykom badającym terroryzm lub jego finansowanie, a dane finansowe nie mogą być łączone z żadną inną bazą danych. Generalnie dane finansowe otrzymane od SWIFT muszą zostać usunięte nie później niż pięć lat po ich otrzymaniu. Dane finansowe, które są istotne dla konkretnych dochodzeń lub operacji ścigania, mogą być zatrzymywane nie dłużej, niż jest to konieczne do celów tych dochodzeń lub operacji ścigania.

Departament Skarbu USA może przekazać informacje pochodzące z danych otrzymanych od SWIFT konkretnym organom ścigania, organom odpowiedzialnym za zapewnienie bezpieczeństwa publicznego lub zwalczanie terroryzmu na terenie Stanów Zjednoczonych bądź poza nimi wyłącznie do celów zapobiegania terroryzmowi, dochodzeń w sprawie terroryzmu, wykrywania bądź ścigania terroryzmu lub jego finansowania. W przypadku gdy dalsze przekazanie danych finansowych dotyczy obywatela lub rezydenta państwa członkowskiego UE, każde udostępnienie danych organom państwa trzeciego jest uzależnione od uprzedniej zgody właściwych organów danego państwa członkowskiego. Wyjątki można uczynić w przypadkach, w których udostępnienie danych ma istotne znaczenie dla zapobieżenia nagłemu i poważnemu zagrożeniu bezpieczeństwa publicznego.

Transfer danych na podstawie umów międzynarodowych – SWIFT / TFTP

Przestrzeganie zasad umowy TFTP monitorują niezależni obserwatorzy, w tym osoba wyznaczona przez Komisję Europejską.

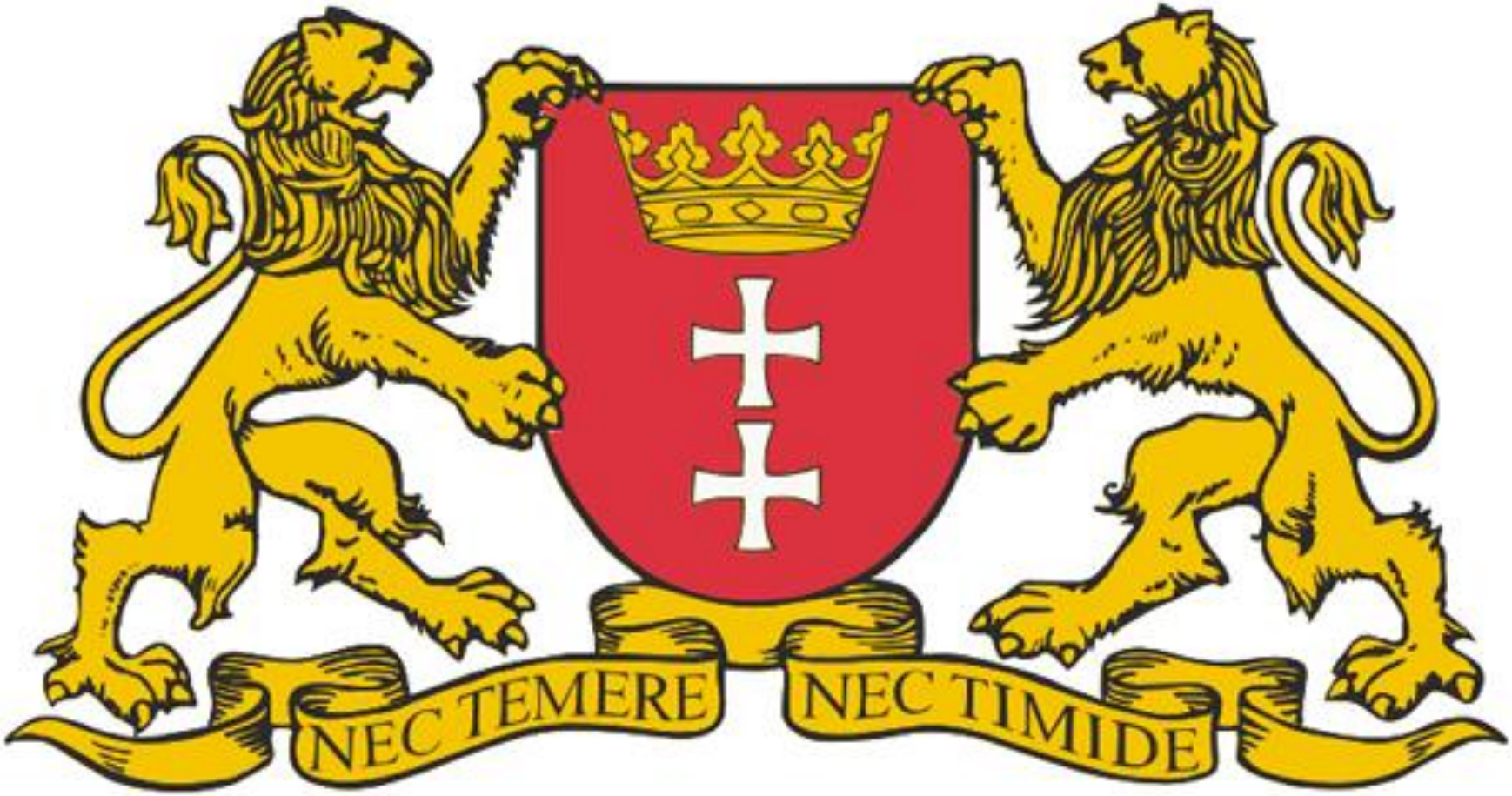
Osoby, których dane dotyczą, mają prawo uzyskać od właściwego urzędu ochrony danych w UE potwierdzenie, że ich prawa do ochrony danych osobowych są przestrzegane. Osoby, których dane dotyczą, mają również prawo poprawienia, usunięcia lub zablokowania swoich danych gromadzonych i przechowywanych przez Departament Skarbu USA na mocy umowy SWIFT. Prawa dostępu osób, których dane dotyczą, mogą jednak podlegać pewnym ograniczeniom prawnym. W przypadku odmowy dostępu osoba, której dane dotyczą, musi zostać poinformowana w formie pisemnej o odmowie oraz przysługującym jej prawie do administracyjnych i sądowych środków zaskarżenia w Stanach Zjednoczonych.

Umowa SWIFT obowiązywała przez pięć lat, do sierpnia 2015 r. Jej okres obowiązywania jest odtąd automatycznie przedłużany na kolejne okresy roczne, chyba że jedna ze stron zawiadomi drugą z przynajmniej sześciomiesięcznym wyprzedzeniem, że nie zamierza przedłużyć okresu obowiązywania umowy.

Informacyjne „samookreślenie” oznacza, że

to MY musimy działać

a nie „oni”


NEC TEMERE
NEC TIMIDE

Dziękuję za uwagę!

=> Q&A <=

Europejski Inspektor Ochrony Danych:
www.edps.europa.eu
edps@edps.europa.eu
@EU_EDPS