



Sesja II - „Ryzyko w ochronie danych osobowych”

Mariola Więckowska

Administrator Bezpieczeństwa Informacji

Allegro

XII DZIEŃ OCHRONY DANYCH OSOBOWYCH

ZANWESTUJ W PRYWATNOŚĆ – PRZYGOTOWUJEMY SIĘ DO #RODO

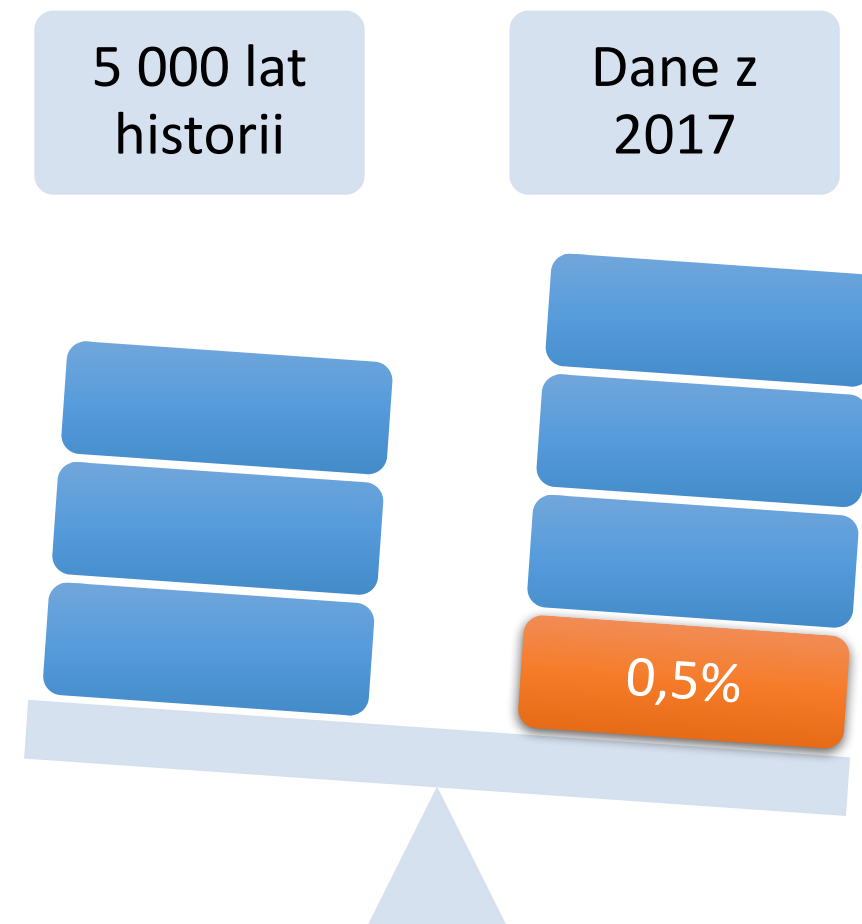
Agenda

- O co tyle hałasu?
- Ryzyko w RODO
- Podejście oparte na ryzyku w organizacji

O co tyle hałasu?

- **16,3 ZB** (zettabajtów) jest przetwarzanych w świecie (1 ZB = 931 322 574 615,48 GB)*
- International Data Corporation szacuje, że w 2020 roku transakcje biznesowe B2B i B2C osiągną **450 miliardów** na dzień
- Akamai analizuje **75 milionów** zdarzeń dziennie, aby lepiej targetować reklamę
- Mniej niż 0,5% danych jest używana do podejmowania decyzji

* Źródło: IDC's Data Age 2025 study, sponsored by Seagate, April 2017,
<https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf>



Naruszenia danych w pierwszym półroczu 2017

Kradzież tożsamości

Kradzież tożsamości stanowiła 74% wszystkich wycieków danych w pierwszej połowie 2017, to 49% więcej w porównaniu z drugą połową 2016.

Wyciek danych medycznych

Ze wszystkich sektorów, wycieki danych z sektora służby zdrowia stanowiły 25% wszystkich wycieków, z największym z brytyjskiej służby zdrowia (National Health Service)

Wycieki danych edukacyjnych

Ten sektor doświadczył 13% ze wszystkich wycieków, co stanowiło przyrost o 103%

Źródło: Breach Level Index by Gemalto, <http://breachlevelindex.com/>

Statystyki: naruszenia danych

Co sekundę

- 122 rekordów danych ulega wyciekowi na świecie (nie wliczając danych z wycieku w Equifax)

Co minutę

- Ponad 7000 rekordów danych jest kradzione lub utracone na świecie, co daje więcej niż 10 milionów każdego dnia.

W pierwszej
połowie
tego roku

- 1,9 miliarda rekordów danych wyciekło w wyniku naruszeń. To drastyczny wzrost o 164% w porównaniu z drugą połową 2016.

Źródło: Breach Level Index by Gemalto, <http://breachlevelindex.com/>

Nearly half of business owners have been victims of cyberattacks



Computer virus
36%



Phishing
29%



Trojan horses
13%



Hacking
12%



Data breach
7%



Ransomware
7%



Issues due to unpatched software
7%



Unauthorized access to company info
7%



Unauthorized access to customer info
6%

Source: Nationwide's third annual survey of business owners.

STEP 1

Create online identity on one or more social networks.

STEP 2

Download potential victim audience with broadcast mechanisms like hashtags. Exploit reputation and reach of relevant influencers by monitoring their follower lists and posting and commenting on their public content.

STEP 3

Directly engage with sympathetic targets through @mention or DM. Encourage them to personally contact you off-platform through text message, phone call or other social media.

STEP 4

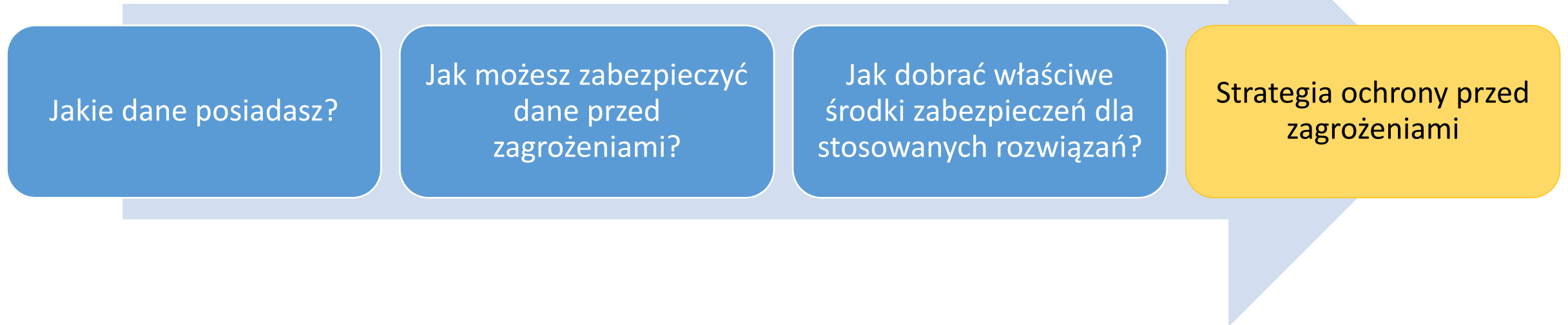
Socially engineer victim through 1:1 conversation to surrender PI, money or credentials.

FIGURE 1:

Spray-and-Pray victim acquisition funnel.



3 kroki do ochrony przed incydentami bezpieczeństwa



- Nieco poniżej 20% utraty lub wycieku danych było spowodowane wewnątrz organizacji – człowiek najłabszym punktem ochrony.
- Szyfrowanie pozostaje brakującym elementem ochrony danych: **mniej niż 1% danych skradzionych w pierwszej połowie 2017 było zaszyfrowanych**. To stanowi znaczne **obniżenie w porównaniu do 4% w drugiej połowie 2016 roku**.
- Odzyskanie stanu sprzed cyberataku jest zwykle powolne i drogie. 20% ofiar ataków wydało na to co najmniej \$50 000 i poświęciło więcej, niż 6 m-cy, zaś 7% wydało ponad \$100 000 i poświęciło więcej niż rok.

Źródło: Breach Level Index by Gemalto, <http://breachlevelindex.com/>

Podejście oparte na ryzyku

Ocena skutków dla Ochrony Danych (OSOD)

Wstępna ocena skutków dla
ochrony danych –
ogólna ocena ryzyka

A. Ocena skutków dla ochrony
danych - analiza zmiany i jej
wpływ na prywatność

Monitoring
wdrożenia

B: Analiza ryzyka i
rekomendowane środki zaradcze

C: Raport końcowy wraz ze
strategią postępowania z
ryzykiem

Ryzyko w RODO



Ryzyko naruszenia praw lub wolności osób, w tym

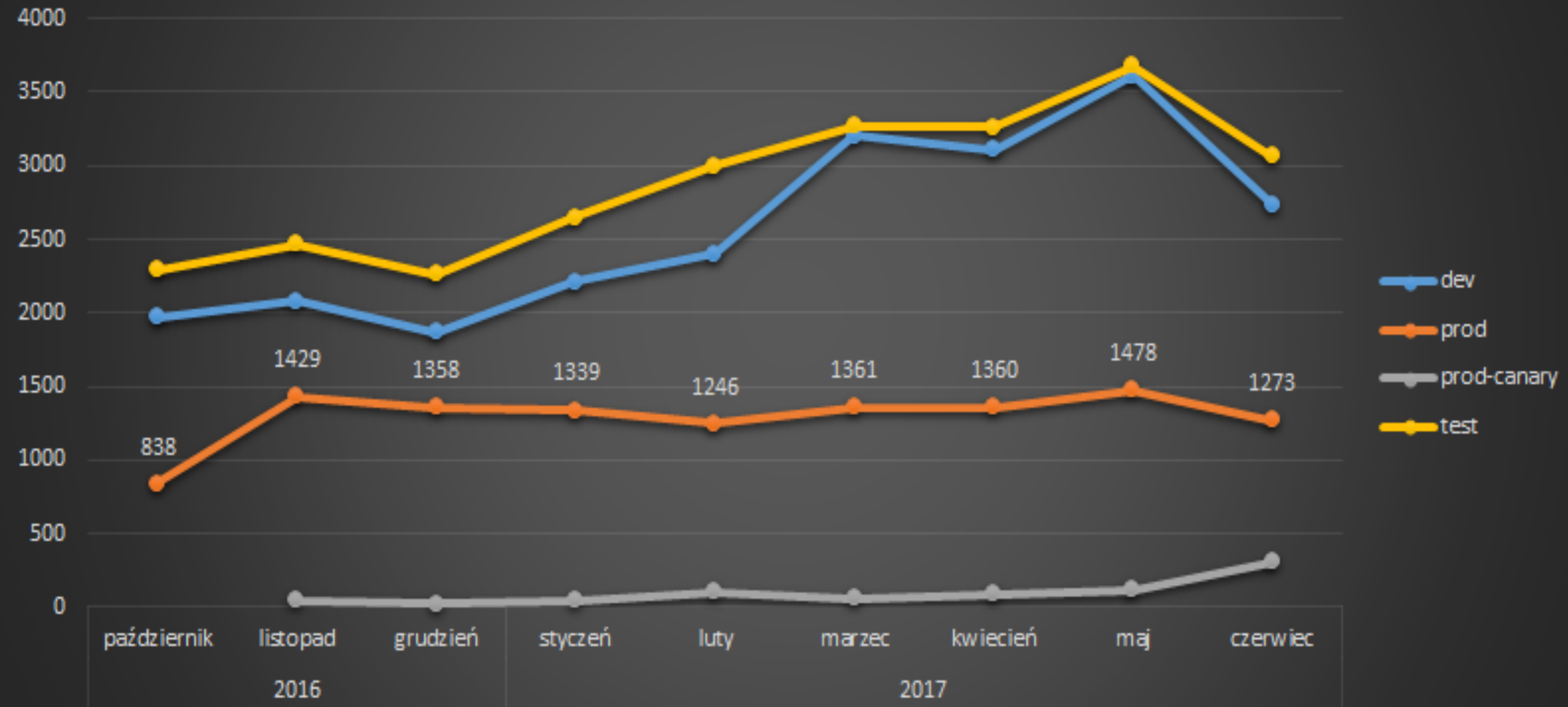
braku wypełniania praw osób, możliwości kradzieży tożsamości, naruszenia dobrego imienia, dyskryminacji lub negatywnych skutków finansowych, pozbawienie przysługujących podmiotom danych ich praw.

Ryzyko wiążące się z przetwarzaniem danych

rodzące skutki finansowe, prawne i utraty reputacji w wyniku naruszenia prywatności;

przypadkowe lub niezgodnego z prawem zniszczenie, utrata, modyfikacja, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Wdrożenia per środowisko Allegro.pl



Analizuj ryzyko już w fazie projektowania



Przestanki do analizy ryzyka ogólnego

Powierzenia przetwarzania danych innym podmiotom

Nowy system informatyczny

Powstanie nowej bazy danych/mikro usługi

Przekazywanie danych do hurtowi danych lub innych wewnętrznych systemów

Udostępnianie/zmiana API wystawianego na zewnątrz firmy

Udostępnienie danych innym podmiotom

Przetwarzanie istniejących danych w nowym celu lub gdy dochodzi do profilowania podmiotu danych

Nowy system monitoringu

Zastosowanie nowej technologii w istniejącym systemie

RYZIKO WYSOKIE => OSOD



Systematyczne monitorowanie

Dokonano porównania lub połączenia zestawów danych

Dane wrażliwe - szczególne kategorie danych w tym dane dotyczące wyroków i naruszeń prawa.

Dane przetwarzane na dużą skalę.

Dane dotyczące osób wymagających szczególnej opieki/dzieci.

Transgraniczne przekazywanie danych

Stosowanie innowacyjnych rozwiązań technologicznych

Przetwarzanie uniemożliwia osobom wykonywanie ich praw lub korzystania z usługi lub umowy

Profilowanie, ocenianie, różnych aspektów dotyczących podmiotów danych

Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne czy inne istotne skutki



Brak
inwentaryzacja
danych i ich
przepływu
między
systemami

Nawet
najlepsze
zabezpieczenia
mają słabe
ogniwo:
człowiek

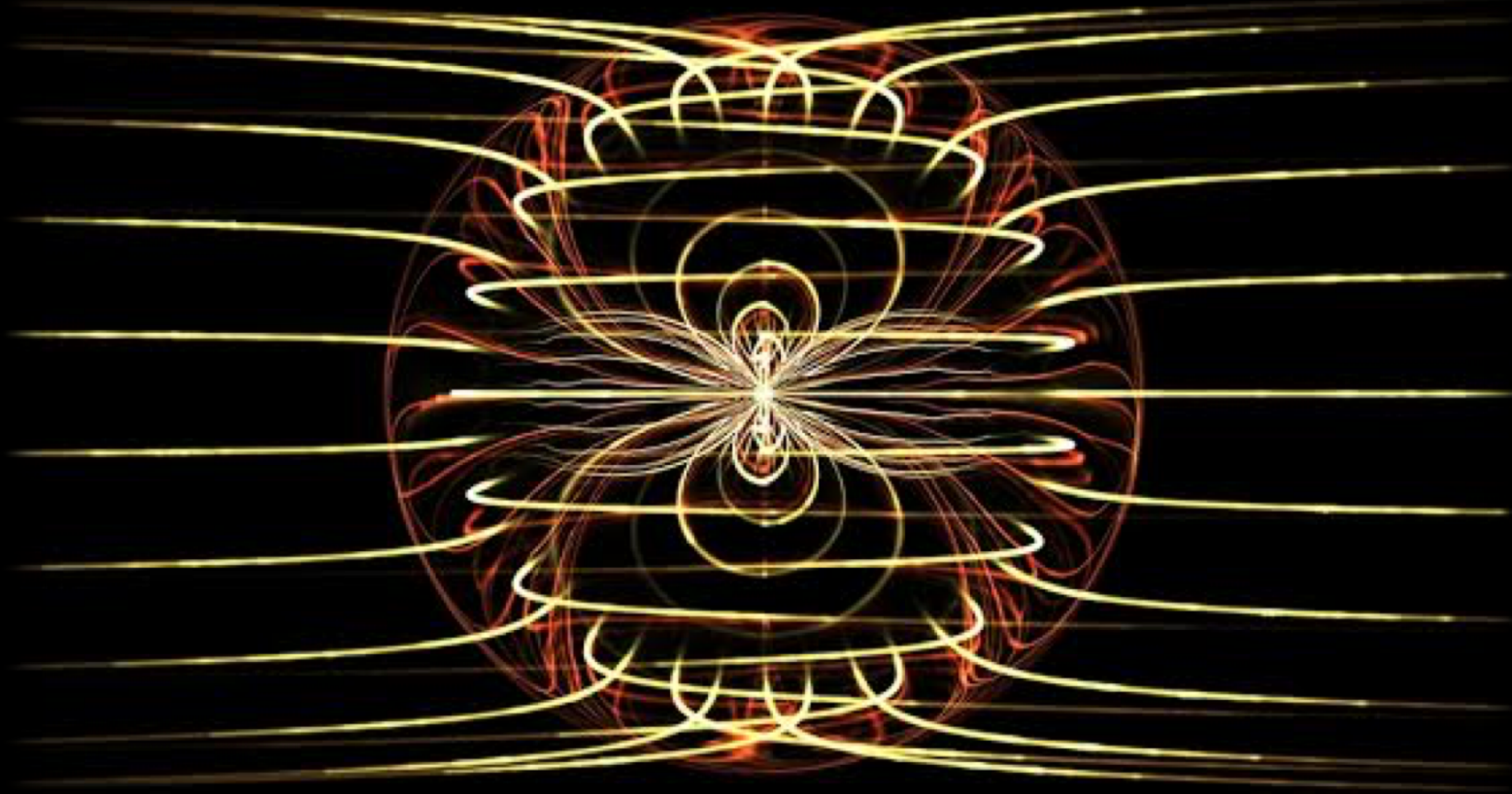


Brak
identyfikacji
wszystkich
systemów z
danymi
osobowymi

Rozliczalność-
czy wystarczy
do wykazania
zgodności z
RODO



Zainwestuj w prywatność!
Warto być na bieżąco ... nadciąga era komputerów kwantowych



E: Mariola.Wieckowska@Allegro.pl

Dziękuję