



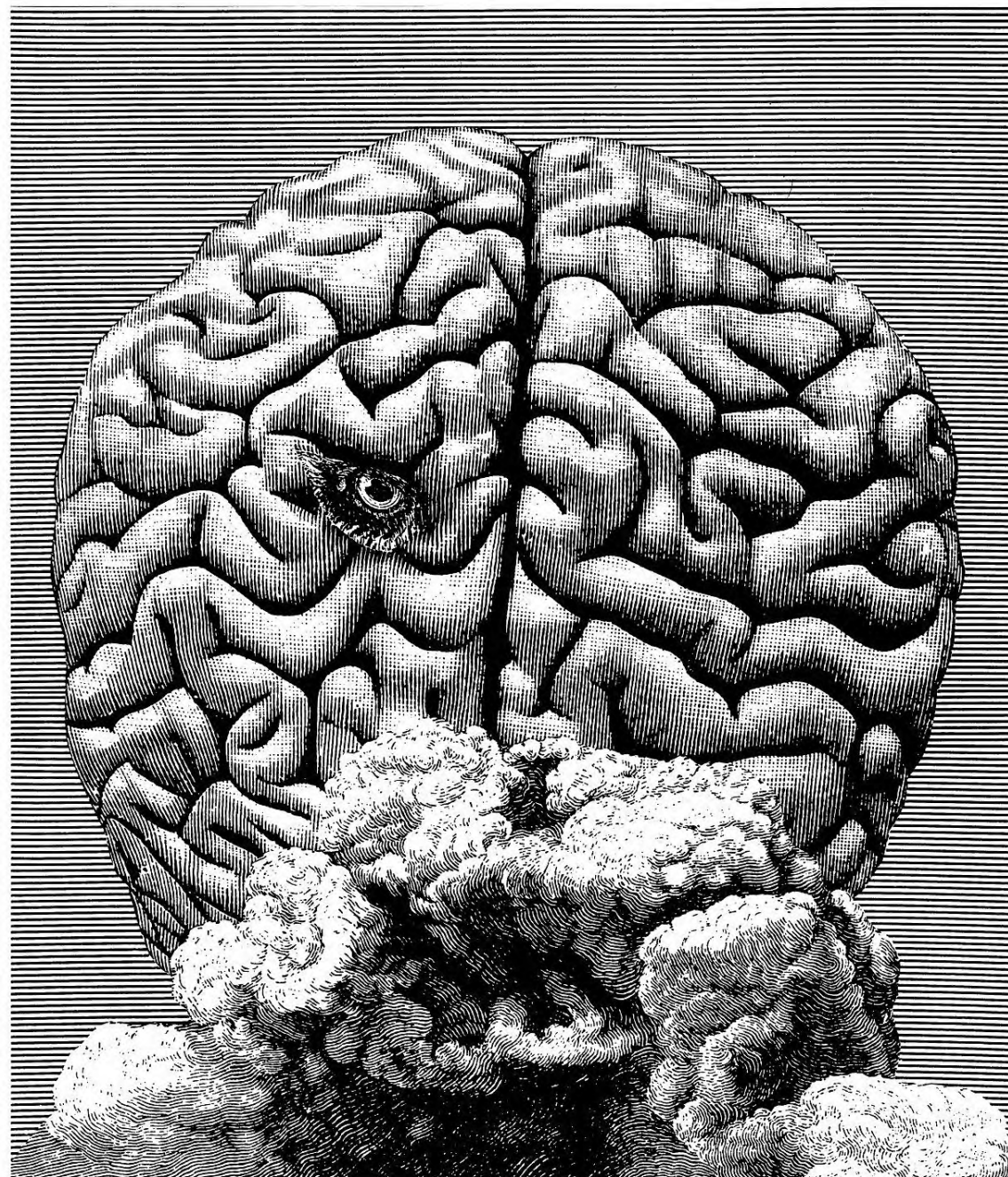
Gawroński & Partners

Rola szyfrowania w zapewnianiu zgodności

adw. Michał Ćwiakowski

Konferencja UODO - Szyfrowanie

Warszawa, 19 lipca 2021 r.



G+P Czy szyfrowanie jest niezbędne do zapewnienia zgodności?

- Tj. czy istnieje prawny obowiązek szyfrowania?
- Bezpieczeństwo vs koszty / wydajność / nakład pracy
- „Niech prawnik rozstrzygnie”
- „A co jest w regulacjach? Musimy szyfrować?”



- Jeden z nielicznych środków technicznych sugerowany wprost w regulacji – art. 32 ust. 1 lit. a RODO:
pseudonimizacja i szyfrowanie danych osobowych

(art. 4 pkt 5 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;

ANALIZA RYZYKA

Art. 32 ust. 1 RODO

Uwzględniając:

- **Stan wiedzy technicznej** (*state of the art*),
- koszt wdrażania,
- Charakter, zakres, kontekst, cele przetwarzania (np. kategorie i skala przetwarzanych danych, powierzenie przetwarzania, długość łańcucha podmiotów przetwarzających)
- **ryzyko naruszenia praw lub wolności osób fizycznych** o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia

administrator i podmiot przetwarzający wdrażają **odpowiednie środki techniczne i organizacyjne**, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku

Decyzja o wdrożeniu środków technicznych polegających na szyfrowaniu cd.

ZAGROŻENIA

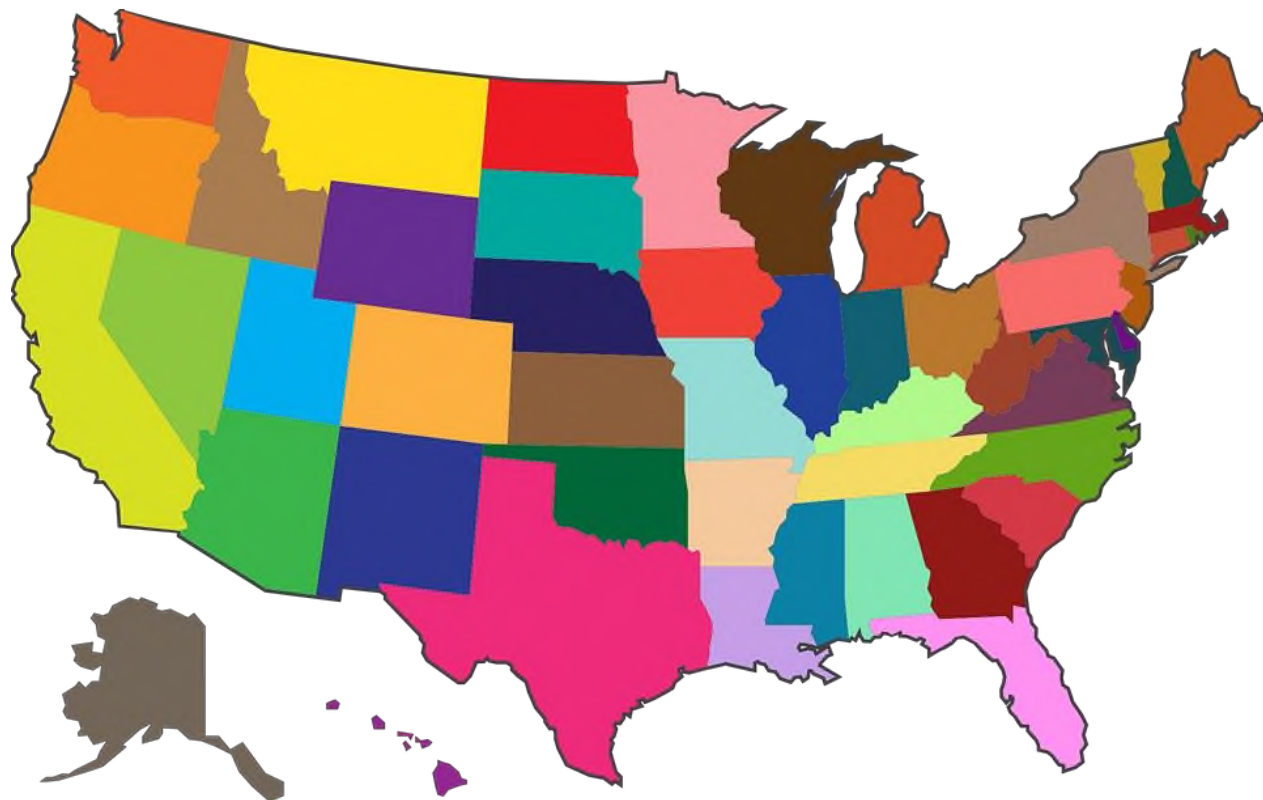
CIA – poufność, integralność, dostępność

Art. 32 ust. 2 RODO

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z:

- przypadkowego lub niezgodnego z prawem zniszczenia,
 - utraty,
 - modyfikacji,
 - nieuprawnionego ujawnienia lub
 - nieuprawnionego dostępu do danych osobowych
- przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Szyfrowanie jako *state of the art*



G+P Szyfrowanie jako *state of the art* cd.

Rekomendowane/wymagane wprost w przepisach prawa, *soft law* lub pozaprawnych standardach, m.in.:

- Wytyczne organów – np. EROD lub sektorowych - KNF, EBA
- Kodeksy postępowania (np. EU Data Protection Code of Conduct for Cloud Service Providers)
- ENISA
- OWASP
- Normy ISO



EU Data Protection Code of Conduct for Cloud Service Providers

„To ensure compliance of a Cloud Service to the security requirement of the Code, the CSP must achieve, at least, the security objectives listed below (*minimalne wymagania techniczne*)

(...)

Where technically feasible and operationally practicable (including based on the nature of the Cloud Service), the CSP shall make available and/or implement encryption controls – at least for any transit of data – to protect the confidentiality of Customer Personal Data in the cloud, where provided for in the Cloud Services Agreement or where considered necessary based on a risk analysis.

Komunikat Chmurowy KNF (VI.2.5.d oraz e)

d) informacje przetwarzane w chmurze obliczeniowej powinny być szyfrowane **zawsze, gdy to jest technologicznie możliwe i – w ocenie podmiotu nadzorowanego – ekonomicznie zasadne**;

e) informacje prawnie chronione **muszą być szyfrowane zawsze „at rest” oraz „in transit”**. Nadzór dopuszcza sytuację, w której informacje prawnie chronione są szyfrowane „at rest” natychmiast po ich przesłaniu do chmury obliczeniowej przy założeniu jednoczesnego stosowania szyfrowania „in transit” i nie traktuje takiej sytuacji jako ujawnienia przetwarzanych informacji;

Projekt Dyrektywy NIS 2 (art. 18)

Użycie metod kryptograficznych i szyfrowania jako wymagane minimum

1. Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented.

*2. The measures referred to in paragraph 1 shall include **at least the following***

(...)

g) the use of cryptography and encryption.

Projekt Dyrektywy NIS 2 postuluje ograniczenia w dopuszczalności wdrażania szyfrowania typu *end-to-end* przez dostawców usług komunikacji elektronicznej

Motyw 54:

Z jednej strony promuje wdrażanie szyfrowania *end-to-end*: *In order to safeguard the security of electronic communications networks and services, **the use of encryption, and in particular end-to-end encryption, should be promoted and, where necessary, should be mandatory** for providers of such services and networks in accordance with the principles of security and privacy by default and by design*

Z drugiej strony: *The use of end-to-end encryption should be reconciled with the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law. Solutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime.*



Krytyczna opinia EIOD - opinia 5/2021 – dotyczące Strategii Cyberbezpieczeństwa i Dyrektywy NIS 2 z 11 marca 2021 r.:

- EIOD postuluje zmianę motywu 54 i wskazanie, że żadne z postanowień dyrektywy nie powinno być interpretowane jako postulat osłabiania szyfrowania typu *end-to-end* za pomocą rozwiązań typu *backdoor* lub innych podobnych.
- EIOD przypomina, że szyfrowanie:
 - Jest podstawowym i **niezastępowalnym** środkiem technicznym służącym ochronie danych osobowych
 - Każde osłabienie mechanizmów szyfrowania (np. obligatoryjne mechanizmy typu *backdoor*) pozbawia szyfrowanie skuteczności, ze względu chociażby na ryzyko bezprawnego wykorzystania
 - Ma podstawową rolę w zapewnianiu zgodności transferów poza EOG



Księga Bezpieczeństwa w komunikacji elektronicznej w pracy Radcy Prawnego.

Dostępna pod adresem: <https://kirp.pl/ksiega-bezpieczenstwa-juz-dostepna/>

Nasza kompleksowa analiza zagadnień bezpieczeństwa wykorzystania popularnych komunikatorów, w tym prawnych aspektów szyfrowania *end-to-end*, transferów danych etc.



G+P Inne aspekty zgodności w kontekście szyfrowania

Zarządzanie łańcuchem outsourcingowym:

Zaszyfrowane dane nie tracą przymiotu danych osobowych

ale

- Potencjał w ograniczeniu dostępu poddostawców do danych osobowych (podpowierzenia) w usługach chmurowych
- Usługi kolokacji?

Zarządzanie transferami danych poza EOG

- Rekomendacje EROD 01/2020 post Schrems II – dodatkowe środki uzupełniające narzędzia tranferu – wdrożenie **szyfrowania typu *end-to-end*** uniemożliwiającego dostęp organów publicznych, w tym wcześniej importera np. operatora usługi chmurowej.



G+P Inne aspekty zgodności w kontekście szyfrowania – c.d.

Kluczowe czynniki:

- *disk encryption vs object encryption (w tym client-based encryption)*
- zarządzanie, generowanie, dostarczanie kluczy kryptograficznych

Czy istnieje zatem obowiązek szyfrowania?

Przepisy prawa + *state of the art* + mnogość mitygowanych ryzyk

Incydent + związek przyczynowo-skutkowy z **brakiem środków technicznych** związanych z **szyfrowaniem**

=

odpowiedzialność

Z pomocą GDPR Enforcement Tracker (<https://www.enforcementtracker.com/>):

<https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/> - administrator przechowywał hasła użytkowników w postaci niaszyfrowanego zwykłego tekstu

<https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf> – kara dla British Airways, dane kart płatniczych przechowywane w formie niaszyfrowanej

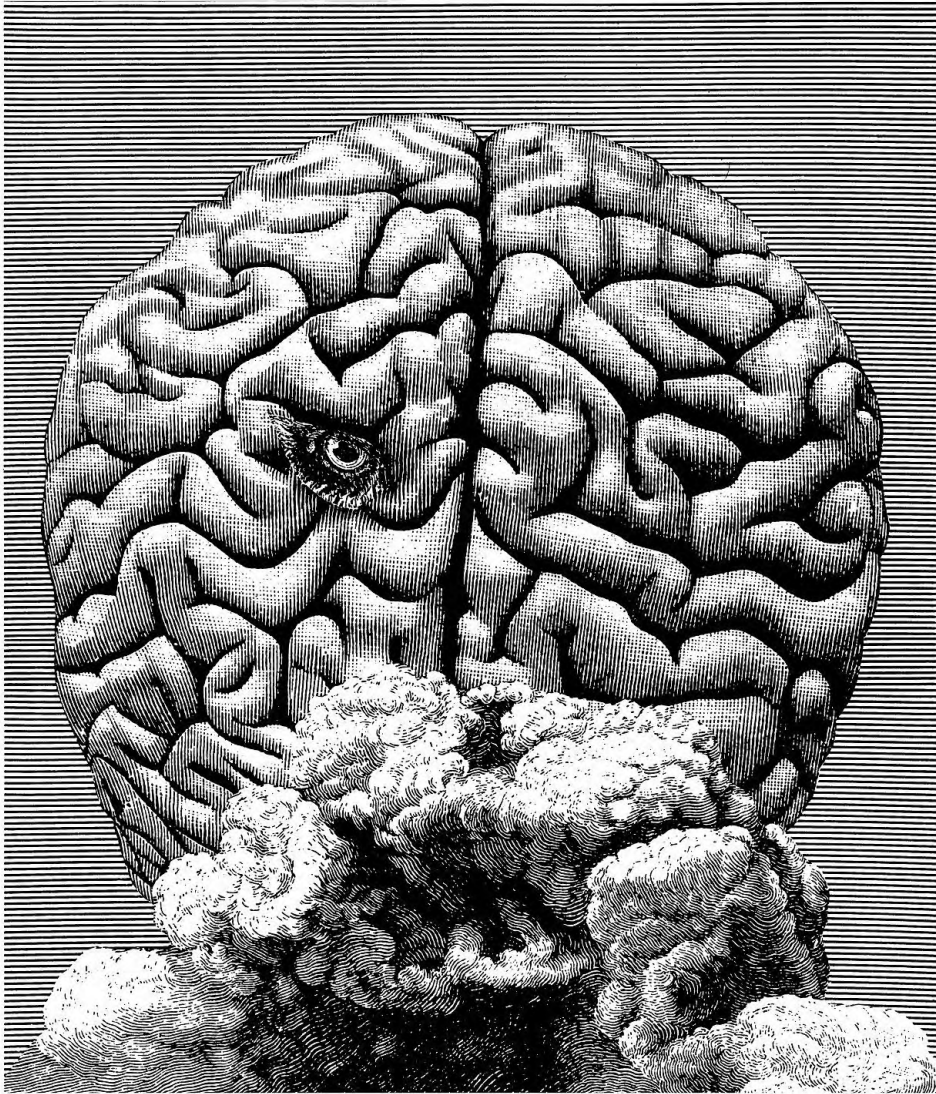
DZIĘKUJEMY ZA UWAGĘ





Michał Ćwiakowski

- Michał Ćwiakowski kieruje zespołem sektora finansowego w Gawroński & Partners a wraz z Maciejem Gawrońskim odpowiada też za praktykę technologii. Doświadczony ekspert w doradztwie dla instytucji finansowych. Pracował w największych bankach w Polsce, zarówno w obszarze prawnym, jak i ryzyka, a następnie w wiodących polskich kancelariach prawnych.
- adwokat, certyfikowany Audytor Wiodący ISO 27001, wykładowca studiów podyplomowych compliance w Szkole Głównej Handlowej
- Doradza podmiotom regulowanym rynku finansowego we wszystkich aspektach ich działalności, m. in. w zakresie AML, usług płatniczych, regulacji bankowych, ładu korporacyjnego, relacji z regulatorem i postępowaniach licencyjnych.
- Doradza klientom również w obszarach związanych z ochroną danych osobowych oraz wdrażaniem i wykorzystaniem nowych technologii. Odpowiedzialny za wsparcie prawne w pionierskich wdrożeniach outsourcingu chmurowego, w tym w sektorze finansowym, kontraktowanie usług z zakresu IT, doradztwo na rzecz podmiotów z sektora e-commerce.
- Doświadczenie zdobyte na rynku finansowym skutecznie przenosi także do innych sektorów. Michał doradza przedsiębiorcom z różnych branż i sektorów, również tym mniejszym, w budowie skutecznych systemów compliance, w oparciu o najlepsze praktyki, skrojone do potrzeb danego klienta, zaczerpnięte przede wszystkim z sektora bankowego – należącego do najbardziej uregulowanych w gospodarce.
- Wszechstronne wykształcenie pozwala mu zrozumieć specyfikę i potrzeby klientów.



© Daniel Mróz

Gawroński & Partners

- niezależna polska firma prawnicza
- zespół dynamicznych ludzi
- doskonali w sektorach regulowanych
- dostarczamy rozwiązania
- pomagamy tworzyć standardy
- w sporach totalnie nieszablonowi



Gawroński & Partners



**RODO
Przewodnik ze wzorami**
Redakcja
Maciej Gawroński



Ochrona danych osobowych
Przewodnik po ustawie i RODO z wzorami
Redakcja
Maciej Gawroński



Guide to the GDPR

June 2019



Pan Maciej Gawroński zajmuje się problematyką z zakresu przetwarzania danych osobowych w chmurze (cloud computing), cyberbezpieczeństwa, IT i własności intelektualnej, którego znaczenie doceniają krajowe i międzynarodowe rankingi prawnicze, wymieniając go wśród wiodących specjalistów prawa z wymienionych dziedzin. Jego doświadczenie zostało również docenione przez instytucje europejskie, z którymi współpracował jako ekspert Komisji Europejskiej do spraw umów o przetwarzaniu danych w chmurze oraz konsultant Grupy Roboczej Art. 29, obecnie zastąpionej przez EROD. Jest autorem wielu naukowych i praktycznych opracowań z zakresu ochrony danych osobowych, które regularnie publikuje w kraju i za granicą.

**Maciej
Gawroński**



Gawroński & Partners Sp.K.

info@gppartners.pl

Al. Jana Pawła II 12, 00-124 Warszawa

