

Wdrażanie SI w organizacji

bezpłatny webinar

RZECZOWO O PRAWIE

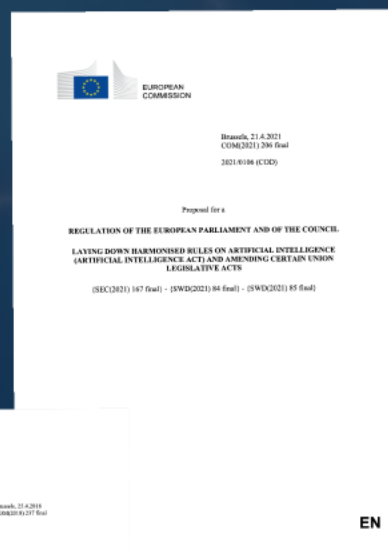
**dr Dominik
Lubasz**

W lubasz&wspólnicy
KANCELARIA RADCÓW PRAWNYCH

Badania prowadzące do powstania referatu zostały sfinansowane przez Narodowe Centrum Nauki w ramach realizacji projektu badawczego „Ochrona konsumenta a sztuczna inteligencja. Między prawem a etyką” (nr projektu: 2018/31/B/HS5/01169).

SI w UE

Skoordynowane podejście do SI



EUROPEAN
COMMISSION

Brussels, 7.12.2018
COM(2018) 795 final

ION FROM THE COMMISSION TO THE EUROPEAN
EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN
SOCIAL COMMITTEE AND THE COMMITTEE OF THE
REGIONS

Coordinated Plan on Artificial Intelligence



Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

**LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE
(ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION
LEGISLATIVE ACTS**

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}



Brussels, 21.4.2021
COM(2021) 205 final
ANNEX

ANNEXES

to the
Communication from the Commission to the European Parliament, the European
Council, the Council, the European Economic and Social Committee and the Committee
of the Regions

Fostering a European approach to Artificial Intelligence

CONTENTS

**COORDINATED PLAN ON ARTIFICIAL INTELLIGENCE
2021 REVIEW**

INTRODUCTION: CREATING EU GLOBAL LEADERSHIP IN HUMAN-CENTRIC AI WITH MEMBER STATES.....	2
I. SET ENABLING CONDITIONS FOR AI DEVELOPMENT AND UPTAKE IN THE EU.....	5
1. Acquire, pool and share policy insights.....	6
2. Tap into the potential of data.....	12
3. Foster critical computing capacity.....	14
II. MAKE THE EU THE PLACE WHERE EXCELLENCE THRIVES FROM THE LAB TO THE MARKET.....	16
4. Collaborate with stakeholders through, e.g. the European Partnership on AI, Data and Robotics and expert groups.....	17
5. Build and mobilise research capacities.....	19

EN

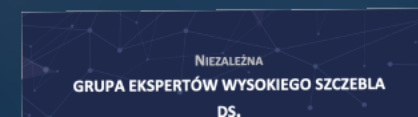
EN



Brussels, 25.4.2018
COM(2018) 237 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN

EN



Godna zaufania sztuczna inteligencja

Zgodna z prawem

Solidna

1. Przewodnia i nadzorczą rolę człowieka
2. Techniczna solidność i bezpieczeństwo
3. Ochrona prywatności i zarządzanie danymi
4. Przyszłość
5. Różnorodność, niedyskryminacja i sprawiedliwość
6. Dobrostan społeczny i środowiskowy
7. Odpowiedzialność

Etyczna

1. Poszanowanie godności człowieka
2. Zapobieganie szkodom
3. Sprawiedliwość
4. Możliwość wyjaśnienia



Godna zaufania sztuczna inteligencja

**Zgodna z
prawem**

Solidna

1. Przewodnia i nadzorcza rola człowieka
2. Techniczna solidność i bezpieczeństwo
3. Ochrona prywatności i zarządzanie danymi
4. Przejrzystość
5. Różnorodność, niedyskryminacja i sprawiedliwość
6. Dobrostan społeczny i środowiskowy
7. Odpowiedzialność

Etyczna

1. Poszanowanie godności człowieka
2. Zapobieganie szkodom
3. Sprawiedliwość
4. Możliwość wyjaśnienia



Etyczna

1. Poszanowanie godności człowieka
2. Zapobieganie szkodom
3. Sprawiedliwość
4. Możliwość wyjaśnienia

Solidna

1. Przewodnia i nadzorczą rolę człowieka
2. Techniczna solidność i bezpieczeństwo
3. Ochrona prywatności i zarządzanie danymi
4. Przejrzystość
5. Różnorodność, niedyskryminacja i sprawiedliwość
6. Dobrostan społeczny i środowiskowy
7. Odpowiedzialność

Wdrażanie SI w organizacji

bezpłatny webinar

RZECZOWO O PRAWIE

dr Dominik
Lubasz

W lubasz&wspólnicy
KANCELARIA RADCÓW PRAWNYCH

Badania prowadzące do powstania referatu zostały sfinansowane przez Narodowe Centrum Nauki w ramach realizacji projektu badawczego „Ochrona konsumenta a sztuczna inteligencja. Między prawem a etyką” (nr projektu: 2018/31/B/HS5/01169).

Risk-based approach

Założenia regulacyjne

14. Aby wprowadzić proporcjonalny i skuteczny zestaw wiążących zasad dotyczących systemów sztucznej inteligencji, należy zastosować jasno określone podejście **oparte na analizie ryzyka**.

Takie podejście powinno polegać na **dostosowywaniu rodzaju i treści takich zasad do intensywności i zakresu zagrożeń**, jakie mogą powodować systemy sztucznej inteligencji.

Risk-based approach

Założenia regulacyjne

14. Aby wprowadzić proporcjonalny i skuteczny zestaw wiążących zasad dotyczących systemów sztucznej inteligencji, należy zastosować jasno określone podejście **oparte na analizie ryzyka**.

Takie podejście powinno polegać na **dostosowywaniu rodzaju i treści takich zasad do intensywności i zakresu zagrożeń**, jakie mogą powodować systemy sztucznej inteligencji.

Wdrażanie SI w organizacji

bezpłatny webinar

RZECZOWO O PRAWIE

**dr Dominik
Lubasz**

W lubasz&wspólnicy
KANCELARIA RADCÓW PRAWNYCH

Badania prowadzące do powstania referatu zostały sfinansowane przez Narodowe Centrum Nauki w ramach realizacji projektu badawczego „Ochrona konsumenta a sztuczna inteligencja. Między prawem a etyką” (nr projektu: 2018/31/B/HS5/01169).

Podejście oparte na ryzyku

Założenia i problemy

1. Horyzontalność regulacji
2. Regulacja produktowa
3. Podmioty zobowiązane - dostawca jako podstawowy podmiot zobowiązany według KE
4. Kwalifikacja systemów SI od grup ryzyk o charakterze *ex ante*
5. Kontekst - FRIA
6. Relacja do RODO



System SI

Zakres i charakter systemu - kwalifikacja systemu

„system sztucznej inteligencji” (wersja PE) oznacza **system maszynowy**, który został zaprojektowany do działania **z różnym poziomem autonomii** i który może – do wyraźnych lub dorozumianych celów – **generować wyniki**, takie jak przewidywania, zalecenia lub decyzje wpływające na środowiska fizyczne lub wirtualne;

System sztucznej inteligencji wysokiego ryzyka:

- a)** system sztucznej inteligencji jest przeznaczony do wykorzystywania jako związany z bezpieczeństwem element produktu objętego unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku II lub sam jest takim produktem;
- b)** produkt, którego związany z bezpieczeństwem elementem jest system sztucznej inteligencji, lub sam system sztucznej inteligencji jako produkt podlegają – na podstawie unijnego prawodawstwa harmonizacyjnego wymienionego w załączniku II – ocenie zgodności przeprowadzanej przez osobę trzecią w celu wprowadzenia tego produktu do obrotu lub oddania go do użytku.

System SI

Zakres i charakter systemu - kwalifikacja systemu

„model generatywny” (wersja PE) oznacza model systemu sztucznej inteligencji, który jest trenowany na szerokiej skali danych, jest zaprojektowany z myślą o ogólnym charakterze wyników i może być dostosowany do szerokiego zakresu odrębnych zadań;

„system sztucznej inteligencji ogólnego przeznaczenia” (wersja PE) oznacza system sztucznej inteligencji, który może być wykorzystywany i dostosowany do szerokiego zakresu zastosowań, do których nie został celowo i specjalnie zaprojektowany;

System SI jako produkt

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Tekst mający znaczenie dla EOG.)

systemy sztucznej inteligencji stwarzające ryzyko rozumie się jako produkt stwarzający ryzyko związane z zagrożeniem dla zdrowia i bezpieczeństwa lub praw podstawowych obywateli.

konsekwencje takiego ujęcia to:

- **kwalifikacja systemów według ryzyk** (systemy zakazane, wysokiego ryzyka, systemy ogólnego ryzyka)
- **ocena *ex ante***
- ocena **oderwana od kontekstu użytkowania**

Dostawca/Użytkownik/ Operator SI

Kwalifikacja zależna od roli i fazy

„**dostawca**” oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które **opracowują system sztucznej inteligencji lub zlecają jego opracowanie w celu wprowadzenia go do obrotu lub oddania go do użytku pod własną nazwą handlową lub własnym znakiem towarowym** – odpłatnie lub nieodpłatnie;

„**użytkownik**” (**operator sztucznej inteligencji**) oznacza osobą fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które **korzystają z systemu sztucznej inteligencji pod swoją kontrolą**, z wyjątkiem sytuacji, gdy system sztucznej inteligencji jest wykorzystywany w ramach osobistej działalności pozazawodowej;

Praktyki zakazane

czarna lista

- a) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu sztucznej inteligencji, który stosuje **techniki podprogowe będące poza świadomością danej osoby w celu istotnego zniekształcenia zachowania tej osoby w sposób**, który powoduje lub może powodować u niej lub u innej osoby szkodę fizyczną lub psychiczną;
- b) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu sztucznej inteligencji, który **wykorzystuje dowolne słabości określonej grupy** osób ze względu na ich wiek, niepełnosprawność ruchową lub zaburzenie psychiczne **w celu istotnego zniekształcenia zachowania osoby należącej do tej grupy w sposób**, który powoduje lub może powodować u tej osoby lub u innej osoby szkodę fizyczną lub psychiczną;
- c) wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemów sztucznej inteligencji **przez organy publiczne lub w ich imieniu na potrzeby oceny lub klasyfikacji wiarygodności osób fizycznych** prowadzonej przez określony czas na podstawie ich zachowania społecznego lub znanych bądź przewidywanych cech osobistych lub cech osobowości, kiedy to punktowa ocena społeczna prowadzi do jednego lub obu z następujących skutków:
 - d) wykorzystywania **systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym” w przestrzeni publicznej do celów egzekwowania prawa**,

Zasady ogólne systemów SI

Wszystkie systemy (Wersja PE)

- a) **„przewodnia i nadzorczą rolę człowieka”** oznacza, że systemy sztucznej inteligencji należy opracowywać i wykorzystywać jako narzędzia służące ludziom, szanujące godność ludzką i autonomię osobistą oraz działające w sposób, który może być odpowiednio kontrolowany i nadzorowany przez człowieka;
- b) **„techniczna solidność i bezpieczeństwo”** oznacza, że systemy sztucznej inteligencji należy opracowywać i wykorzystywać tak, aby minimalizować niezamierzone i nieoczekiwane szkody, a także tak, aby były one solidne w przypadku niezamierzonych problemów i odporne na próby zmiany ich zastosowania lub skuteczności działania umożliwiające ich wykorzystanie przez działające w złej wierze strony trzecie;
- c) **„prywatność i zarządzanie danymi”** oznacza, że systemy sztucznej inteligencji należy opracowywać i wykorzystywać zgodnie z obowiązującymi przepisami dotyczącymi prywatności i ochrony danych, a jednocześnie należy przetwarzać dane spełniające wysokie standardy pod względem jakości i integralności;
- d) **„przejrzystość”** oznacza, że systemy sztucznej inteligencji należy opracowywać i wykorzystywać w sposób umożliwiający odpowiednią identyfikowalność i wytłumaczalność, przy jednoczesnym informowaniu ludzi o tym, że komunikują się z systemem sztucznej inteligencji lub podejmują z nim interakcję, a także przy należytym informowaniu użytkowników o możliwościach i ograniczeniach tego systemu sztucznej inteligencji, a osób, których to dotyczy, o przysługujących im prawach;
- e) **„różnorodność, niedyskryminacja i sprawiedliwość”** oznacza, że systemy sztucznej inteligencji należy opracowywać i wykorzystywać w sposób, który angażuje różne podmioty i propaguje równy dostęp, równouprawnienie płci i różnorodność kulturową, a jednocześnie należy unikać dyskryminujących skutków zakazanych prawem Unii lub prawem krajowym;
- f) **„dobrostan społeczny i środowiskowy”** oznacza, że systemy sztucznej inteligencji należy opracowywać i wykorzystywać w sposób zrównoważony, przyjazny dla środowiska i przynoszący korzyści wszystkim ludziom, a jednocześnie należy monitorować i oceniać ich długoterminowy wpływ na jednostkę, społeczeństwo i demokrację.

Wymogi systemów SI wysokiego ryzyka

1. System zarządzania ryzykiem
2. Dane i zarządzanie danymi
3. Dokumentacja techniczna
4. Rejestrowanie zdarzeń
5. Przejrzystość i udostępnianie informacji użytkownikom
6. Nadzór ze strony człowieka
7. Dokładność, solidność i cyberbezpieczeństwo

Obowiązki dostawcy

1. Zapewnienie zgodności z wymogami
2. Dokumentacja techniczna
3. Systemy zarządzania jakością
4. Obowiązki rejestracyjne (art. 51)
5. Poddanie systemu SI procedurze oceny zgodności
6. Automatycznie generowane rejestry zdarzeń
7. Działania naprawcze
8. Współpraca z organami

Obowiązki dostawcy modelu generatywnego

1. Wykazuje – poprzez odpowiednie **projektowanie, testowanie i analizę** - że identyfikowano, ograniczano i łagodząco racjonalnie przewidywalne **zagrożenia** dla zdrowia, bezpieczeństwa, praw podstawowych, środowiska, demokracji i praworządności
2. przetwarza i uwzględnia wyłącznie te **zbiory danych**, które podlegają odpowiednim środkom zarządzania danymi w zakresie modeli generatywnych, w szczególności środkom mającym na celu zbadanie **adekwatności źródeł danych i możliwej tendencyjności** oraz działań łagodzących w tym zakresie;
3. projektuje i rozwija model generatywny tak, aby osiągnąć w całym jego cyklu życia odpowiednie poziomy **skuteczności działania, przewidywalności, interpretowalności, korygowalności, bezpieczeństwa i cyberbezpieczeństwa**, które są oceniane za pomocą adekwatnych metod

Obowiązki dostawcy modelu generatywnego

4. projektuje i rozwija model generatywny z uwzględnieniem mających zastosowanie norm w celu ograniczenia zużycia energii, zużycia zasobów i odpadów, a także zwiększenia efektywności energetycznej i ogólnej efektywności systemu, bez uszczerbku dla odpowiednich obowiązujących przepisów unijnych i krajowych (**cele zrównoważonego rozwoju**)
5. sporządza obszerną **dokumentację techniczną i zrozumiałe instrukcje** użytkowania
6. ustanawia **system zarządzania jakością**
7. **rejestruje** model generatywny w unijnej bazie danych

Obowiązki użytkownika/ operatora SI

1. Zapewnienie użytkowania zgodnie z instrukcją
2. Wdrażanie rozwiązań zapewniających nadzór człowieka
3. Sprawowanie kontrole nad danymi wejściowymi, zapewnienie adekwatność i wystarczającej reprezentatywność danych wejściowych (wersja PE)
4. Obowiązki monitorowania i informowania dostawców o ryzyku
5. Prowadzenie rejestry zdarzeń
6. Obowiązki konsultacyjne z przedstawicielami pracowników (wersja PE)
7. Obowiązki informacyjne dotyczące niektórych systemów w zakresie dotyczącym interakcji z SI
8. Przeprowadzanie oceny skutków dla praw podstawowych (FRIA) (wersja PE)

Fundamental rights impact assessment

Przed oddaniem do użytku systemu sztucznej inteligencji **wysokiego ryzyka** określonego w art. 6 ust. 2, z wyjątkiem systemów sztucznej inteligencji przeznaczonych do użytku w obszarze 2 załącznika III, **operatorzy sztucznej inteligencji** przeprowadzają **ocenę skutków systemu w szczególnym kontekście jego wykorzystania**, zawierającą

- a) jasne informacje o **przeznaczeniu** systemu,
- b) jasne informacje o **geograficznym i czasowym zakresie wykorzystania** systemu,
- c) **kategorie osób fizycznych i grup**, na które wykorzystanie systemu może mieć **wpływ**,
- d) **weryfikację zgodności wykorzystania** systemu z prawem unijnym i krajowym oraz z prawami podstawowymi,
- e) dający się **racjonalnie przewidzieć wpływ** oddania do użytku systemu sztucznej inteligencji wysokiego ryzyka **na prawa podstawowe**,
- f) szczególne **ryzyko wystąpienia szkód**, które mogą mieć wpływ na **osoby zmarginalizowane lub grupy szczególnie wrażliwe**,
- g) dający się racjonalnie przewidzieć **negatywny wpływ korzystania z systemu na środowisko**,
- h) szczegółowy **plan określający sposób ograniczania szkód i negatywnego wpływu** na prawa podstawowe,
- j) **system zarządzania**, jaki wprowadzi operator sztucznej inteligencji, w tym **nadzór ludzki, rozpatrywanie skarg i środki odwoławcze**

Fundamental rights impact assessment

Assessment List for Trustworthy Artificial Intelligence

ALTAI to stworzone i opublikowane przez Grupę Ekspertów wysokiego szczebla ds. sztucznej inteligencji (AI HLEG) <https://futurium.ec.europa.eu/en/european-ai-alliance/pages/welcome-altai-portal>

Nadzór człowieka
Solidność techniczna i bezpieczeństwo
Prywatność i zarządzanie danymi
Przejrzystość
Różnorodność, niedyskryminacja i sprawiedliwość
Dobrostan środowiskowy i społeczny
Rozliczalność

Wdrażanie SI w organizacji

bezpłatny webinar

RZECZOWO O PRAWIE

**dr Dominik
Lubasz**

W lubasz&wspólnicy
KANCELARIA RADCÓW PRAWNYCH

Badania prowadzące do powstania referatu zostały sfinansowane przez Narodowe Centrum Nauki w ramach realizacji projektu badawczego „Ochrona konsumenta a sztuczna inteligencja. Między prawem a etyką” (nr projektu: 2018/31/B/HS5/01169).

Relacja AIA - RODO

Założenia Komisji Europejskiej

Zapewnia się **spójność** z Kartą praw podstawowych UE oraz obowiązującym unijnym **prawem wtórnym w zakresie ochrony danych, ochrony konsumentów, niedyskryminacji i równouprawnienia płci**.

Wniosek pozostaje **bez uszczerbku dla przepisów i uzupełnia ogólne rozporządzenie o ochronie danych (rozporządzenie (UE) 2016/679)** o zestaw zharmonizowanych przepisów mających zastosowanie do projektowania, opracowywania i stosowania niektórych systemów **AI wysokiego ryzyka** oraz ograniczeń dotyczących niektórych zastosowań systemów zdalnej identyfikacji biometrycznej.

Relacja AIA - RODO

Podjęcie Parlamentu Europejskiego

Art. 2 ust. 5a prawo Unii w zakresie ochrony danych osobowych, prywatności i poufności komunikacji **ma zastosowanie** do danych osobowych przetwarzanych w związku z prawami i obowiązkami określonymi w niniejszym rozporządzeniu.

Niniejsze rozporządzenie **nie ma wpływu na rozporządzenia (UE) 2016/679** i (UE) 2018/1725 ani na dyrektywy 2002/58/WE i (UE) 2016/680, z zastrzeżeniem ustaleń przewidzianych w art. 10 ust. 5 i art. 54 niniejszego rozporządzenia



Analiza *fit for purpose* RODO

Cele i cechy rozporządzenia:

- zapewnienie wysokiego poziomu ochrony praw osób fizycznych
- podejście neutralne technologicznie,
- implementacja wymogów opiera się na analizie ryzyka (*risk-based approach*),
- elementami prawidłowego wdrożenia rozporządzenia są nie tylko zagadnienia bezpieczeństwa przetwarzania, lecz także zasady przetwarzania.

Szczegółne rozwiązania regulacyjne:

- obowiązek uwzględniania ochrony danych w fazie projektowania (***data protection by design*** – art. 25 ust. 1 RODO) oraz
- domyślna ochrona danych (*data protection by default* – art. 25 ust. 2 RODO),
- zautomatyzowane podejmowanie decyzji - art. 22 RODO
- oceny skutków przetwarzania dla ochrony danych (*data protection impact assessment* – art. 35 RODO) .

Obowiązki z RODO

Obowiązki przy opracowywaniu i aplikacji systemów SI



Zgodność z zasadami przetwarzania



Weryfikacja podstaw przetwarzania



Realizacja praw podmiotów danych



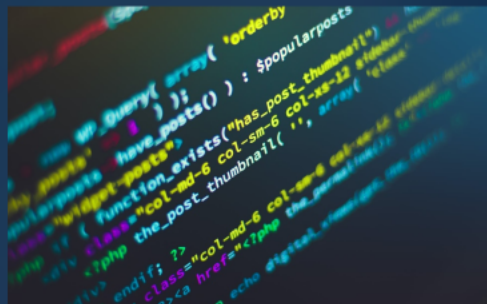
DPIA



Kontekstowa analiza ryzyka



Zapewnienie bezpieczeństwa



Wdrożenie przy uwzględnieniu data protection by design



Zasada rozliczalności

Privacy by design by Ann Cavoukian



- 1) proaktywnym podejściu, a nie reaktywnym i zaradczym, nie naprawczym;
- 2) prywatności jako ustawieniu domyślnym;
- 3) prywatności włączonej w projekt;
- 4) pełnej funkcjonalności rozumianej jako osiągnięcie sumy dodatniej, nie sumy zerowej;
- 5) ochronie prywatności od początku do końca cyklu życia informacji;
- 6) transparentności i przejrzystości;
- 7) poszanowaniu dla prywatności użytkowników.

Art. 25 ust. 1 RODO

Uwzględnianie ochrony danych w fazie projektowania (*data protection by design*)



- 1) Założeniem jest ochrona również proaktywna i prewencyjna
- 2) Element projektu równoważny z celami biznesowymi
- 3) Analiza ma charakter kontekstowy
- 4) Realizowany etapowo
- 5) Wnioski oparte są na analizie ryzyka poprzedzonej analizą zgodności z zasadami przetwarzania, zwłaszcza zasadą minimalizacji i przejrzystości oraz analizą zapewnienia realizacji praw podmiotów danych

Data protection by design - fazy wdrożenia



Źródło: Opracowanie norweskiego organu nadzorczego ds. ochrony danych osobowych Software development with Data Protection by Design and by Default <https://www.datatilsynet.no/en/about-privacy/virksohmhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true>

Zasady przetwarzania danych



Zasada zgodności z prawem i rzetelności

Weryfikacja podstaw prawnych oraz respektowanie praw podmiotów danych, zautomatyzowane podejmowanie decyzji



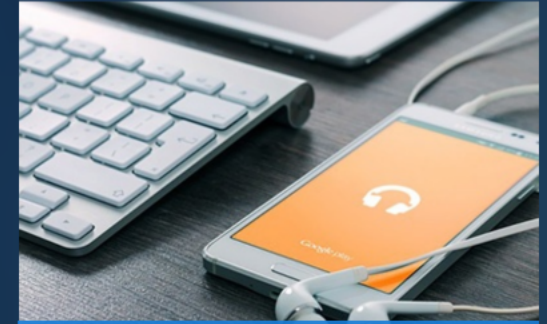
Zasada przejrzystości

Zakres informacji. Informacja o algorytmie? Jak działa SI?



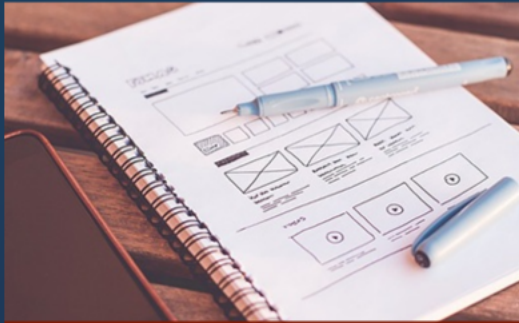
Zasada ograniczenia celu

Wykorzystanie danych do karmienia mechanizmów samouczących, testów i badań.



Zasada minimalizacji danych

Jak dużo danych potrzeba by SI działało? Jak zapewnić rozliczalność modelu - problem nieprzewidywalności efektu?



Zasada ograniczenia przechowywania

Przechowywanie na wszelki wypadek? Rozwój narzędzia?



Zasada prawidłowości

Efekt wnioskowania jako dane osobowe - problem kwestionowania prawidłowości działania.



Zasada poufności i integralności

Data protection by design jako element budowy systemów SI bazujący na ocenie ryzyka.



Zasada rozliczalności

Wykaż zgodność!

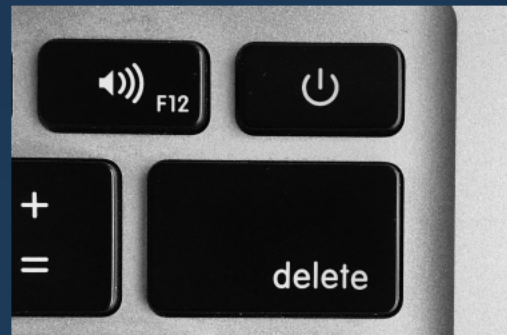
Prawa podmiotów danych



Prawa informacyjne



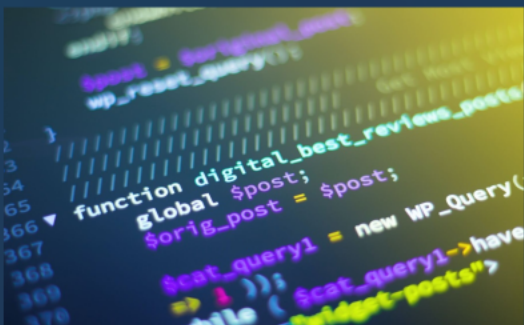
Prawa dostępowe



Prawo do usunięcia



Prawo do sprostowania



Prawo ograniczenia



Prawo sprzeciwu



Prawo do przenoszenia



Zautomatyzowane
podejmowanie decyzji

Bezpieczeństwo



Proaktywna identyfikacja zagrożeń dla bezpieczeństwa, minimalizacja zagrożeń, techniczna solidność

Czynniki wpływające na bezpieczeństwo:

- 1)** sposób, w jaki technologia jest budowana i wdrażana;
- 2)** złożoność organizacji ją wdrażającej;
- 3)** siłę i dojrzałość istniejących możliwości w zakresie zarządzania ryzykiem;
- 4)** charakter, zakres, kontekst i cele przetwarzania danych osobowych przez system SI oraz związane z tym ryzyko dla osób fizycznych.

Data protection by design - fazy wdrożenia



Źródło: Opracowanie norweskiego organu nadzorczego ds. ochrony danych osobowych Software development with Data Protection by Design and by Default <https://www.datatilsynet.no/en/about-privacy/virksohmhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true>

Relacja AIA - RODO

W kontekście analizy ryzyka

1. Brak relacji *lex generalis - lex specialis*
2. Możliwy *overlapping*
3. Weryfikacja z perspektywy zasad przetwarzania i praw podstawowych
4. Odmienność perspektywy oceny dla dostawców i operatorów SI - zagadnienia kontekstowe
5. Wątpliwości terminologiczne



Wdrażanie SI w organizacji

bezpłatny webinar

RZECZOWO O PRAWIE

**dr Dominik
Lubasz**

W lubasz&wspólnicy
KANCELARIA RADCÓW PRAWNYCH

Badania prowadzące do powstania referatu zostały sfinansowane przez Narodowe Centrum Nauki w ramach realizacji projektu badawczego „Ochrona konsumenta a sztuczna inteligencja. Między prawem a etyką” (nr projektu: 2018/31/B/HS5/01169).

Dziękuję za uwagę
dr DOMINIK LUBASZ
radca prawny



dominik.lubasz@lubasziwspolnicy.pl



[www.facebook.com/
/dominik.lubasz](https://www.facebook.com/dominik.lubasz)



lubasziwspolnicy.pl



[www.linkedin.com/
in/dominik-lubasz](https://www.linkedin.com/in/dominik-lubasz)



509 824 632

Wdrażanie SI w organizacji

bezpłatny webinar

RZECZOWO O PRAWIE

**dr Dominik
Lubasz**

W lubasz&wspólnicy
KANCELARIA RADCÓW PRAWNYCH

Badania prowadzące do powstania referatu zostały sfinansowane przez Narodowe Centrum Nauki w ramach realizacji projektu badawczego „Ochrona konsumenta a sztuczna inteligencja. Między prawem a etyką” (nr projektu: 2018/31/B/HS5/01169).