

Wykaz skrótów .....	17
<b>Wprowadzenie</b> .....	21
<b>Rozdział I</b> .....	
<b>Regulacja technologii</b> .....	29
1. Regulacja innowacji .....	30
1.1. Regulacja neutralna technologicznie i specyficzna technologicznie .....	31
1.2. Neutralność wobec funkcjonalnie równoważnych technologii.....	34
1.3. Neutralność w kontekście rozwoju technologii .....	36
<b>Rozdział II</b> .....	
<b>Geneza AI Act</b> .....	39
1. Publiczna konsultacja w zakresie przyszłości robotyki i sztucznej inteligencji .....	41
2. Komunikat w sprawie sztucznej inteligencji dla Europy .....	44
2.1. Wzmacnianie potencjału technologicznego i przemysłowego w obszarze AI .....	45
2.2. Przygotowanie się na zmiany społeczno-ekonomiczne .....	47
3. Zapewnienie właściwych ram etycznych i prawnych .....	48
3.1. Projekt wytycznych ws. godnej zaufania AI.....	48
3.2. Bezpieczeństwo i odpowiedzialność.....	49
3.3. Wzmocnienie pozycji konsumentów i użytkowników .....	50
3.4. Najważniejsze działania Komisji.....	50
4. Współpraca państw członkowskich i interesariuszy – skoordynowany plan i Europejski Sojusz na rzecz Sztucznej Inteligencji .....	51
5. Skoordynowany plan w sprawie sztucznej inteligencji .....	52
6. Godna zaufania sztuczna inteligencja .....	56
6.1. Podstawy godnej zaufania sztucznej inteligencji – prawa podstawowe i zasady etyczne dla AI.....	57
6.2. Tworzenie godnej zaufania sztucznej inteligencji.....	61

7.	Konieczność regulacji AI .....	65
8.	Europejska strategia cyfrowa i danych.....	67
9.	Podsumowanie procesu legislacyjnego – Biała księga AI .....	69
10.	Ekosystem doskonałości – ramy polityki dla sztucznej inteligencji.....	70
11.	Ekosystem zaufania.....	71
	Sztuczna inteligencja a problem odpowiedzialności.....	72
12.	Wizja europejskiej regulacji AI .....	74
13.	Negocjacje trójstronne.....	77
14.	Kluczowe sporne kwestie w procesie legislacyjnym.....	78
	14.1. Modele bazowe – generatywna AI .....	78
	14.2. Zdalna biometryczna identyfikacja w czasie rzeczywistym .....	79
	Negocjacje nad definicją AI.....	79
15.	Cele AI Act .....	80

### Rozdział III

<b>Zakres stosowania .....</b>	<b>83</b>
1. Zakres materialny. Które systemy są objęte AI Act? .....	84
1.1. Definicja systemu AI .....	84
Cel wytycznych .....	85
2. Główne elementy definicji systemu AI.....	85
2.1. System maszynowy.....	85
2.2. Autonomia .....	86
2.3. Adaptacyjność.....	87
2.4. Cele systemu AI .....	88
2.5. Wnioskowanie, jak generować wyniki przy użyciu technik AI.....	89
2.5.1. Techniki AI umożliwiające wnioskowanie .....	89
2.5.2. Kategorie wyników systemu AI .....	92
2.5.3. Wpływ wyników na środowisko fizyczne lub wirtualne .....	93
2.5.4. Systemy poza zakresem definicji systemu AI.....	93
2.6. Systemy do poprawy optymalizacji matematycznej.....	94
2.6.1. Podstawowe przetwarzanie danych.....	95
2.6.2. Systemy oparte na klasycznych heurystykach .....	96
2.6.3. Proste systemy predykcyjne.....	96
2.7. Wyniki, które mogą wpływać na środowiska fizyczne lub wirtualne .....	97
2.8. Uwagi końcowe .....	97
3. Modele sztucznej inteligencji ogólnego przeznaczenia.....	98
Chronione dobra prawne .....	99
4. Zakres podmiotowy stosowania .....	99
5. Strony chronione .....	101
6. Zakres terytorialny stosowania.....	102
Wyłączenia z zakresu stosowania .....	104
7. Zakres wyłączenia dla systemów AI <i>open source</i> .....	104

8.	Geneza regulacji i debata wokół FOSS .....	104
9.	Definicja i charakterystyka FOSS w kontekście AI Act.....	105
10.	Oprogramowanie <i>open source</i> .....	107
10.1.	Systemy AI <i>open source</i> .....	107
10.2.	Modele GPAI <i>open source</i> (OSS AI Components) .....	108
10.3.	GPAI w ekosystemie <i>open source</i> (OSS GPAI Models).....	108
10.4.	Systemowe ryzyko a modele OSS GPAI .....	109
10.5.	Wyłączenia a RODO .....	109
10.5.1.	Wyłączenie dla badań naukowych i rozwoju.....	110
10.5.2.	Wyłączenie dla systemów wojskowych i obronnych.....	111
10.6.	Wyłączenia dodane w procesie legislacyjnym.....	112
	Wyłączenie dla użytkowników indywidualnych.....	113
11.	Odniesienia do innych unijnych aktów prawnych.....	113
12.	Ograniczenia w zakresie czasowym – przepisy przejściowe .....	114
<b>Rozdział IV</b>		
<b>Wymagania ogólne i obowiązki przejrzystości</b> .....		
1.	Wymagania ogólne dla wszystkich systemów AI.....	115
2.	Kompetencje w zakresie AI.....	116
2.1.	Egzekwowanie obowiązku .....	118
2.2.	Realizacja obowiązku.....	120
2.3.	Obowiązki przejrzystości dla niektórych systemów AI i modeli GPAI .....	121
2.4.	Systemy AI z interakcją człowieka .....	122
3.	Oznakowanie mediów generowanych przez AI.....	122
4.	Informacje o rozpoznawaniu emocji i kategoryzacji biometrycznej.....	123
4.1.	Oznaczanie treści zawierających <i>deepfake</i> .....	123
	Systemy AI o podwójnym zastosowaniu.....	124
4.2.	Procedura informacyjna i kodeksy postępowania.....	124
<b>Rozdział V</b>		
<b>Klasyfikacja ryzyka</b> .....		
1.	Uwagi ogólne.....	127
2.	Zakazane praktyki AI.....	130
2.1.	AI wpływające na działania i zachowanie ludzi .....	130
2.2.	W stronę dynamicznego podejścia do zakazanych praktyk .....	131
2.3.	Techniki podprogowe, manipulacyjne lub zwodnicze.....	132
2.4.	Wykorzystywanie podatności.....	134
2.5.	AI kategoryzujące, klasyfikujące i identyfikujące ludzi.....	136
2.5.1.	System wiarygodności społecznej.....	136
2.5.2.	Predykcyjne działania policyjne.....	138
2.5.3.	Zakaz zastosowań biometrycznych – wstęp .....	140

2.5.4.	Tworzenie lub powiększanie zbiorów danych skanów twarzy przez nieselektywne gromadzenie skanów twarzy ...	141
2.5.5.	Rozpoznawanie emocji.....	142
2.6.	Kategoryzacja biometryczna.....	144
3.	Zdalna biometryczna identyfikacja w czasie rzeczywistym.....	146
3.1.	Zgoda sądu lub niezależnego organu.....	147
3.1.1.	Pojęcie niezależności.....	147
3.1.2.	Właściwość miejscowa.....	147
3.1.3.	Konieczność i proporcjonalność.....	148
3.1.4.	Wyjątek.....	148
3.2.	Zakaz podejmowania decyzji wyłącznie na podstawie wyników RBI.....	148
	Obowiązek zgłoszenia każdego użycia systemu RBI do organów nadzorczych.....	149
4.	Dopuszczalne cele stosowania RBI.....	150
4.1.	Poszukiwanie ofiar przestępstw i osób zaginionych.....	150
4.2.	Odpieranie poważnych zagrożeń.....	150
4.3.	Dochodzenie w sprawie przestępstw.....	151
4.4.	Cele inne niż egzekwowanie prawa.....	151
	Dalsze wymogi dotyczące RBI.....	151
4.5.	Ocena wpływu sytuacji.....	152
4.6.	Ocena wpływu interwencji.....	152
4.7.	Odpowiednie ograniczenia, ocena skutków dla praw podstawowych i rejestracja.....	152
4.8.	Zezwolenie na RBI przez organy krajowe.....	152
4.9.	Zawiadamianie organu nadzoru rynku i organu ochrony danych ...	153
4.10.	Implementacja RBI w prawie krajowym.....	153
4.11.	Roczne sprawozdanie organów nadzoru rynku i organów ochrony danych o stosowaniu RBI.....	154
4.12.	Coroczne sprawozdanie Komisji o stosowaniu RBI.....	154
4.13.	Stosunek do innego prawa Unii.....	155
<b>Rozdział VI</b>		
<b>Systemy AI wysokiego ryzyka</b> .....		157
1.	Klasyfikacja systemów wysokiego ryzyka.....	158
2.	Klasyfikacja zgodnie z art. 6 ust. 2 AI Act.....	161
2.1.	Wyjątki od klasyfikacji jako wysokiego ryzyka.....	162
2.2.	Wąsko określone zadanie proceduralne.....	163
2.3.	Ulepszanie rezultatu działań już zakończonych przez człowieka.....	163
2.4.	Analiza wzorców podejmowania decyzji.....	165
2.5.	Zadania przygotowawcze.....	165
2.6.	Wyłączenie z klasyfikacji wysokiego ryzyka.....	166

2.7.	Relacja między wyłączeniem na podstawie art. 6 ust. 3 a zmianą	251
2.8.	przeznaczenia w rozumieniu art. 25 ust. 1 lit. c AI Act.....	167
2.9.	Obowiązek dokumentacji i rejestracji dostawców.....	168
2.9.	Prawo Komisji do zmiany właściwych kryteriów.....	169
13.	Systemy AI wysokiego ryzyka zgodnie z art. 6 ust. 1 w zw.	254
	z załącznikiem I AI Act.....	170
3.1.	Sposoby uznania za system AI wysokiego ryzyka zgodnie	255
	z art. 6 ust. 1 w zw. z załącznikiem I AI Act.....	170
3.2.	Systemy AI wysokiego ryzyka w prawie dotyczącym	256
	bezpieczeństwa produktów.....	171
3.3.	Regulacja produktów w ramach starego porządku prawnego.....	171
3.4.	Prawo Komisji do zmiany załącznika III AI Act.....	172
3.5.	Regulacja produktów w ramach nowych ram legislacyjnych.....	172
3.6.	Konsekwencje zakwalifikowania jako system wysokiego ryzyka.....	173
4.	Systemy AI wysokiego ryzyka zgodnie z art. 6 ust. 2	258
	w zw. z załącznikiem III AI Act.....	174
4.1.	Identyfikacja biometryczna, kategoryzacja i rozpoznawanie	260
	emocji osób fizycznych.....	175
4.2.	Infrastruktura krytyczna.....	178
4.3.	Edukacja i szkolenia.....	180
	4.3.1. Rekomendacje dla instytucji edukacyjnych.....	187
	4.3.2. Reguły ogólne.....	188
	4.3.3. Sztuczna inteligencja w edukacji.....	188
4.4.	Zatrudnienie, zarządzanie pracownikami i dostęp	262
	do samozatrudnienia.....	194
4.5.	Zakres sektorowy.....	194
	4.5.1. Zatrudnienie.....	195
	4.5.2. Dostęp do samozatrudnienia.....	195
	4.5.3. Zarządzanie pracownikami.....	196
	4.5.4. Rekrutacja i wybór kandydatów.....	196
	4.5.5. Warunki zatrudnienia.....	197
4.6.	Zwolnienia z wymogów wysokiego ryzyka.....	198
5.	Dostęp do podstawowych usług i świadczeń prywatnych i publicznych.....	200
	5.1. Dostęp do publicznego wsparcia i usług.....	201
	5.2. Zdolność kredytowa.....	202
	5.3. Ubezpieczenia.....	204
	5.4. Wezwania alarmowe.....	205
	5.5. Ściganie.....	206
	5.6. Migracja, azyl i kontrola graniczna.....	208
	5.7. Wymiar sprawiedliwości i procesy demokratyczne.....	210
6.	Klasyfikacja wysokiego ryzyka zgodnie z załącznikiem III pkt 8.....	210
	6.1. Wymiar sprawiedliwości.....	210
	6.2. Technologie prawnicze.....	214

6.3.	Procesy demokratyczne .....	214
7.	Wymogi dla systemów AI wysokiego ryzyka .....	215
7.1.	Adresaci obowiązków .....	216
	Sposoby zapewnienia zgodności .....	216
7.2.	Szczególne cechy systemów AI w rozumieniu art. 6 ust. 1 .....	217
7.3.	Scenariusze zastosowania i zbieżność z innymi obowiązkami z AI Act .....	218
7.4.	System zarządzania ryzykiem .....	219
7.4.1.	Wymagania z art. 9 wobec systemu zarządzania ryzykiem .....	223
7.4.2.	Dowód spełnienia art. 9 AI Act .....	226
7.5.	Dane i zarządzanie danymi .....	227
7.5.1.	Regulacja zbiorów danych do trenowania, walidacji i testowania .....	229
7.5.2.	Wymogi dotyczące projektowania systemu AI .....	230
7.5.3.	Dane istotne, reprezentatywne i wolne od błędów .....	231
7.5.4.	Uwzględnienie typowych warunków użycia .....	232
7.5.5.	Podstawa prawna do przetwarzania szczególnych kategorii danych osobowych .....	232
7.5.6.	Dane testowe .....	233
7.6.	Dokumentacja techniczna .....	234
7.7.	Obowiązki rejestrowania .....	236
7.7.1.	Funkcje rejestrowania zapewniające możliwość prześledzenia ( <i>traceability</i> ) .....	237
7.7.2.	Szczególne funkcje rejestrowania w systemach zdalnej identyfikacji biometrycznej .....	238
7.7.3.	Adresat i okres przechowywania .....	238
7.7.4.	Konflikt z niezawisłością sędziowską .....	239
7.8.	Przejrzystość i przekazywanie informacji użytkownikom .....	239
7.8.1.	Znaczenie przejrzystości w korzystaniu z systemów AI wysokiego ryzyka .....	240
7.8.2.	Przejrzystość .....	240
7.8.3.	Instrukcje użytkownika .....	241
7.9.	Nadzór ludzki .....	242
7.9.1.	Zrozumienie działania i ryzyk (art. 14 ust. 4 lit. a–c) .....	243
7.9.2.	Możliwość ingerencji w działanie .....	244
7.9.3.	Weryfikacja przy zdalnej identyfikacji biometrycznej .....	245
7.10.	Dokładność, odporność i cyberbezpieczeństwo .....	246
8.	Obowiązki związane z postępowaniem z systemami sztucznej inteligencji wysokiego ryzyka .....	248
8.1.	Obowiązki dostawców systemów AI wysokiego ryzyka .....	248
8.2.	Ogólne obowiązki dostawców .....	248
8.3.	Istnienie systemu zarządzania jakością .....	249

8.4.	Przechowywanie dokumentacji.....	251
8.5.	Zachowywanie logów.....	252
8.6.	Podejmowanie działań naprawczych i obowiązków informacyjny.....	252
8.7.	Współpraca z właściwymi organami.....	253
8.8.	Wyznaczenie upoważnionego przedstawiciela.....	254
8.9.	Obowiązki importerów systemów AI wysokiego ryzyka.....	255
8.9.1.	Obowiązek sprawdzenia.....	255
8.9.2.	Obowiązki po wprowadzeniu na rynek.....	256
8.9.3.	Współpraca z właściwymi organami.....	256
8.10.	Obowiązki dystrybutorów systemów AI wysokiego ryzyka.....	257
8.10.1.	Obowiązek sprawdzenia.....	257
8.10.2.	Obowiązki po udostępnieniu na rynku.....	257
8.10.3.	Współpraca z właściwymi organami krajowymi.....	258
8.11.	Obowiązki użytkowników systemów AI wysokiego ryzyka.....	258
8.11.1.	Obowiązki związane z użytkowaniem.....	258
8.11.2.	Odpowiednie i reprezentatywne dane wejściowe.....	259
8.11.3.	Obowiązki monitorowania.....	260
8.11.4.	Przechowywanie automatycznie generowanych logów.....	260
8.11.5.	Obowiązek informowania pracowników.....	260
8.11.6.	Rejestracja.....	261
8.11.7.	Wykorzystanie informacji dostarczonych przez dostawcę do oceny skutków dla ochrony danych.....	261
8.11.8.	System AI wysokiego ryzyka do następczej (post) zdalnej identyfikacji biometrycznej.....	262
8.11.9.	Obowiązek informowania osób fizycznych.....	263
8.11.10.	Współpraca z właściwymi organami krajowymi.....	264
8.12.	Ocena skutków dla praw podstawowych ( <i>fundamental rights impact assessment</i> ) w odniesieniu do systemów AI wysokiego ryzyka.....	264
8.12.1.	Użytkownicy zobowiązani do przeprowadzenia oceny skutków dla praw podstawowych.....	264
8.12.2.	Czas, częstotliwość przeprowadzania oceny oraz relacja do DPIA.....	264
8.12.3.	Zakres oceny skutków dla praw podstawowych.....	265
8.12.4.	Zawiadomienie organu nadzoru rynku.....	265
8.13.	Systemy AI objęte szczególnymi obowiązkami w zakresie przejrzystości.....	266
8.13.1.	Termin realizacji obowiązków przejrzystości.....	266
8.13.2.	Zgodność z właściwymi wymaganiami dostępności (ust. 5).....	267
8.14.	Szczególne obowiązki przejrzystości.....	267
8.14.1.	Systemy AI przeznaczone do bezpośredniej interakcji z osobami fizycznymi (ust. 1).....	267

8.14.2.	Systemy AI generujące „syntetyczne” nagrania audio, obrazy, wideo lub tekst (ust. 2)	268
8.14.3.	Systemy rozpoznawania emocji lub kategoryzacji biometrycznej (ust. 3)	269
8.14.4.	Systemy AI generujące <i>deepfake</i> (ust. 4 zdanie pierwsze)	270
8.14.5.	System AI generujący lub modyfikujący tekst w celu informowania opinii publicznej (ust. 4 zdanie drugie)	270
8.15.	Relacja szczególnych obowiązków przejrzystości do rozporządzenia o usługach cyfrowych (DSA)	271
8.16.	Proste systemy AI	271
<b>Rozdział VII</b>		
<b>Odpowiedzialność wzdłuż łańcucha wartości AI</b>		273
1.	Problemy koncepcyjne w podejściu regulacyjnym Komisji	273
	Zarys finalnego podejścia po trilogu	276
2.	Modele GPAI obciążone ryzykiem systemowym (poziom 1)	277
2.1.	Geneza	277
2.2.	Definicje modeli GPAI	278
2.3.	Klasyfikacja modeli GPAI o ryzyku systemowym	278
2.4.	GPAI o ryzyku systemowym	278
2.5.	Obowiązek notyfikacji	278
2.6.	Obowiązki informacyjne i dokumentacyjne	279
2.7.	Szczególne obowiązki wobec modeli GPAI o ryzyku systemowym	279
2.8.	Kodeks praktyk dla AI ogólnego przeznaczenia	279
2.8.1.	Kluczowe elementy Kodeksu	280
2.8.2.	Wnioski	282
2.8.3.	Dalsze kroki dotyczące Kodeksu	282
3.	Modele GPAI bez ryzyka systemowego i inne komponenty AI (poziom 2)	283
3.1.	Umieszczanie systemu AI na rynku pod własną nazwą lub marką	286
3.2.	Modyfikacja techniczna systemu	286
3.3.	Zmiana zamierzonego celu ( <i>intended purpose</i> )	287
3.4.	Współpraca	287
3.5.	Obowiązki podmiotów wdrażających systemy	288
4.	Osoba, której dotyczy działanie systemu	289
5.	Standaryzowane normy i wspólne specyfikacje	290
5.1.	Europejska standaryzacja	290
5.2.	Rola standaryzacji w AI Act	291
5.3.	Zharmonizowane normy i dokumenty normalizacyjne	292
5.4.	Wspólne specyfikacje	293
5.5.	Piaskownice regulacyjne	294

5.5.1.	Uwagi ogólne .....	294
5.5.2.	Cele piaskownic regulacyjnych .....	295
5.6.	Akty wykonawcze Komisji .....	296
5.7.	Zezwolenie na dalsze przetwarzanie danych osobowych .....	296
5.8.	Sprawozdanie końcowe .....	297
5.9.	Odpowiedzialność .....	297
5.10.	Testy w warunkach rzeczywistych poza piaskownicami regulacyjnymi AI .....	298
5.11.	Wspieranie innowacji, zwłaszcza wśród MŚP i start-upów .....	299
6.	Krajowe regulacje .....	300
6.1.	Zakres stosowania AI Act .....	301
	Klauzule otwierające (informacyjne) .....	301
6.2.	Dopuszczalność stosowania systemów AI .....	302
<b>Rozdział VIII</b>		
<b>Związek z innymi obszarami prawa .....</b>		
1.	Ochrona danych osobowych – RODO .....	305
1.1.	Zakres stosowania i odpowiedzialność .....	305
1.2.	Kategorie danych przy obchodzeniu się z systemami AI .....	306
1.3.	Zastosowanie RODO .....	306
1.4.	Odpowiedzialność w rozumieniu prawa ochrony danych .....	308
1.5.	Pojęcie sztucznej inteligencji w RODO .....	309
1.6.	Zakaz przetwarzania bez zezwolenia na podstawie art. 6 ust. 1 oraz art. 9 ust. 1 RODO .....	310
1.6.1.	Zgoda .....	310
1.6.2.	Niezbędność dla wykonania umowy .....	311
1.6.3.	Niezbędność dla wypełnienia obowiązku prawnego .....	311
1.6.4.	Interes publiczny lub sprawowanie władzy publicznej .....	312
1.6.5.	Uzasadniony interes .....	312
1.6.6.	Zmiana celu .....	314
1.7.	Szczególne kategorie danych osobowych .....	314
1.8.	Zakaz zautomatyzowanego podejmowania decyzji indywidualnych na podstawie art. 22 RODO .....	315
1.9.	Przejrzystość i obowiązki informacyjne zgodnie z art. 5 ust. 1 lit. a i art. 12 i n. RODO .....	317
1.10.	Środki techniczne i organizacyjne .....	319
1.10.1.	Wymogi RODO .....	320
1.10.2.	Cel środków technicznych i organizacyjnych w RODO .....	320
1.10.3.	Organizacja przetwarzania .....	321
1.10.4.	Bezpieczeństwo przetwarzania .....	322
1.11.	Znaczenie dla systemów AI .....	322
1.11.1.	Realizacja art. 25 RODO w kontekście systemów AI .....	323
1.11.2.	Realizacja art. 32 RODO w kontekście systemów AI .....	324

2.	Akt o usługach cyfrowych .....	325
2.1.	Obszary zastosowania: VLOPs/VLOSEs a systemy wysokiego ryzyka/GPAI.....	326
2.2.	Analiza ryzyka systemowego.....	327
2.3.	Ryzyka systemowe w rozumieniu AI Act i DSA .....	327
2.4.	Zintegrowana i międzytechnologiczna analiza ryzyka .....	328
2.5.	Dostęp dla naukowców .....	329
2.6.	Moderacja treści a art. 55 AI Act.....	330
2.7.	Wynik pośredni dla AI Act i DSA .....	331
3.	Akt w sprawie danych .....	332
3.1.	Uwagi ogólne na temat relacji między AI Act a DA .....	333
3.2.	Dane i zarządzanie danymi .....	334
4.	Akt w sprawie zarządzania danymi (DGA) .....	335
4.1.	Adresaci DGA .....	335
4.2.	Cele AI Act a DGA .....	336
4.2.1.	AI Act – bezpieczeństwo i odpowiedzialność w stosowaniu AI .....	336
4.2.2.	DGA – dostępność i wymiana danych .....	336
4.2.3.	Relacja komplementarna między AI Act a DGA .....	336
5.	Europejskie przestrzenie danych ( <i>European data spaces</i> ) .....	337
5.1.	EPDZ.....	337
5.2.	Prawa osób fizycznych i przetwarzanie wtórne .....	339
5.3.	Zastosowanie równoległe z AI Act.....	339
<b>Rozdział IX</b>		
<b>Instytucjonalne ramy zarządzania .....</b>		
1.	AI Office – centralna instytucja nowego systemu .....	342
1.1.	Struktura i kompetencje .....	342
1.2.	Wyzwania organizacyjne.....	343
2.	Europejska Rada ds. Sztucznej Inteligencji i organy doradcze .....	343
2.1.	Struktura i skład Rady .....	343
2.2.	Zadania i kompetencje.....	343
2.3.	Forum doradcze i panel naukowy.....	344
3.	Organy krajowe i ich rola w systemie .....	344
3.1.	Organy notyfikujące.....	344
3.2.	Jednostki notyfikowane .....	344
3.3.	Organy nadzoru rynku .....	345
4.	Wyzwania koordynacji i współpracy .....	345
4.1.	Koordynacja między poziomami zarządzania.....	345
4.2.	Nakładanie się kompetencji.....	345
4.3.	Rekomendacje dla usprawnienia systemu zarządzania .....	346
4.3.1.	Wyjaśnienie projektu instytucjonalnego AI Office .....	346
4.3.2.	Integracja forum i panelu w jeden organ.....	346

4.3.3.	Ustanowienie centrum koordynacji AI .....	346
4.3.4.	Mechanizmy uczenia się .....	346
4.4.	Przyszłe wyzwania.....	347
4.4.1.	Koordinacja z innymi ramami regulacyjnymi UE .....	347
4.4.2.	Współpraca międzynarodowa .....	347
<b>Wnioski</b> .....		<b>349</b>
1.	Hybrydowa natura AI Act i jej konsekwencje.....	349
2.	Wyzwanie tempa rozwoju technologicznego .....	350
3.	Niedopasowanie środków do celów.....	351
4.	Konsekwencje dziedziczenia instytucjonalnego.....	351
5.	Implikacje systemowe i długoterminowe .....	352
6.	Kierunki reform i rekomendacje.....	353
7.	Perspektywy przyszłościowe.....	354
8.	Refleksje końcowe.....	355
<b>Bibliografia</b> .....		<b>357</b>
	2014/90/UE (UE) 2016/797 i (UE) 2016/1829 (akt w sprawie	
	wzajemnej odpowiedzialności) (Dz.Uz. UE L 2014/168)	
	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/680	
	z 13.12.2016 r. w sprawie zbiorów danych przetwarzanych przez	
	urzędy w celu zapewnienia bezpieczeństwa i ochrony	
	prywatności i w sprawie zmiany rozporządzenia (UE) 2016/1829	
	oraz w sprawie zmiany rozporządzenia (UE) 2016/1829 i dy-	
	rektywy (UE) 2016/1828 (akt w sprawie danych) (Dz.Uz. UE L	
	2016/2854)	
Deklaracja montrealaska	Deklaracja montrealaska na rzecz odpowiedzialnego rozwoju	
	cyfrowej inteligencji, podpisana 3.11.2017 r., <a href="https://montreal-declaration-responsibleai.com/the-declaration/">https://montreal-</a>	
DGA	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2012/368	
	z 10.05.2012 r. w sprawie europejskiego zarządcy danych i	
	funkcjonujące rozporządzenie (UE) 2018/1724 (akt w sprawie za-	
	rzadzania danymi) (Dz.Uz. UE L 153, s. 1, 04 zm.)	
DMA	rozporządzenie Parlamentu Europejskiego i Rady (UE)	
	2022/1925 z 14.09.2022 r. w sprawie kontestowalnych i uczci-	
	wych rynków w sektorze cyfrowym oraz zmian dyrektyw (UE)	
	2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.Uz.	
	UE L 265, s. 1, 26 zm.)	
DSA	rozporządzenie Parlamentu Europejskiego i Rady (UE)	
	2022/2065 z 19.10.2022 r. w sprawie jednolitego rynku usług	
	cyfrowych oraz zmiany dyrektywy 2006/114/WE (akt o usługach	
	cyfrowych) (Dz.Uz. UE L 277, s. 1, 04 zm.)	
dyrektywa maszynowa	dyrektywa 2006/42/WE Parlamentu Europejskiego i Rady	
	z 17.05.2006 r. w sprawie maszyn, zmieniająca dyrektywę	
	90/269/WE (przekształcenie) (Dz.Uz. UE L 157, s. 24, 04 zm.)	
EKPC	Konwencja o ochronie praw człowieka i podstawowych wolno-	
	ści opracowana w Rzymie 4.11.1950 r. (Dz.U. z 1991 r. Nr 61,	
	poz. 284 ze zm.)	
EPDZ	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/327	
	z 11.02.2023 r. w sprawie europejskiej przestrzeni danych doty-	
	czących zdrowia oraz zmiany dyrektywy 2011/24/UE (rozporz-	
	ządzenia (UE) 2023/2647 (Dz.Uz. UE) 2023/327)	