

Spis treści

Wstęp	9
-------	---

CZĘŚĆ I

Systemy AI jako narzędzie biznesowe dla MŚP. Aspekt biznesowy i informatyczny	15
--	----

ROZDZIAŁ 1

Od sztucznej inteligencji do systemów AI – podstawy wdrożeń w biznesie	16
1.1. Merytoryczny fundament wdrożenia: systemy, agenty AI i organizacja <i>data-driven</i>	17
1.1.1. Podstawowe pojęcia związane ze sztuczną inteligencją	18
1.1.2. Czym są agenty AI?	19
1.1.3. Systemy AI i rola danych	21
1.1.4. Ograniczenia AI	21
1.1.5. Zagrożenia AI	22
1.2. Wdrożenie systemu AI – konieczność, a nie opcja	23
1.3. Potencjał biznesowy projektu wykorzystującego system AI	25
1.3.1. Dlaczego trudno wyliczyć zysk z rozwiązań AI?	26
1.3.2. Indeks ROI AI	27
1.4. Rola systemów AI w budowaniu przewagi konkurencyjnej	27
1.5. Czy Twoja firma jest gotowa na wdrożenie systemu AI?	29
1.6. Przegląd zastosowań systemów AI dla MŚP	32
1.7. Najczęściej popełniane błędy przy wdrażaniu systemów AI	36
1.7.1. Błędy prawne	36
1.7.2. Błędy techniczne	43
1.7.3. Błędy biznesowe	46

ROZDZIAŁ 2

Agenty AI na przykładzie projektowania agenta wspomagającego proces rekrutacji	50
2.1. Jak zaprojektować agenta AI?	51
2.1.1. Agent AI jako system zdarzeniowy (<i>event-driven</i>)	51
2.1.2. Zakres autonomii i nadzór człowieka (<i>Human-in-the-Loop</i>)	52
2.1.3. Multiagent jako podział odpowiedzialności	52
2.2. Określenie celu i zakresu działania agenta	53
2.3. Wybór technologii	54
2.3.1. Instrukcje dla LLM jako element konfiguracji systemu AI	57
2.3.2. Integracja z istniejącymi systemami	58
2.4. Budżetowanie i wybór platformy	61
2.5. Cykl życia projektu GenAI	67
2.6. Ryzyka wdrożenia agenta AI i jak im przeciwdziałać	68
2.6.1. Metryki sukcesu i monitorowanie efektywności (przykładowe)	69
2.6.2. Bezpieczeństwo i ochrona danych	70
2.6.3. Zarządzanie błędami i wyjątkami	71
2.7. Wprowadzenie dotyczące wdrożenia agenta AI w procesie rekrutacyjnym (przykład PoC/MVP)	71

CZĘŚĆ II

AI Act RODO i Data Act – jak bezpiecznie zarządzać danymi, by uniknąć milionowych kar	75
--	-----------

ROZDZIAŁ 3

Zanim organizacja podejmie decyzję o wdrożeniu agenta AI	76
3.1. Rola firmy wdrażającej systemy AI na gruncie AI Act i RODO i Data Act	77
3.2. Wysokość ryzyka związanego z systemami AI a obowiązki przedsiębiorcy	86
3.2.1. Systemy zakazane	87
3.2.2. Systemy wysokiego ryzyka	88
3.2.3. Systemy ograniczonego ryzyka	94
3.2.4. Systemy minimalnego ryzyka	97
3.2.5. Modele AI i Systemy AI ogólnego przeznaczenia (GPAI)	98
3.3. Kluczowe obowiązki organizacji korzystających z systemów AI	100
3.3.1. Obowiązki dostawców	105
3.3.2. Obowiązki podmiotów stosujących	116
3.4. Kary administracyjne na podstawie AI Act i RODO	117

ROZDZIAŁ 4

Jak wdrożyć agenta AI zgodnie z przepisami RODO?

Praktyczna dokumentacja	121
4.1. Wykorzystanie danych osobowych – zasada rozliczalności	122
4.1.1. Profilowanie i zautomatyzowane podejmowanie decyzji wobec kandydatów do pracy	127
4.1.2. Transparentność przetwarzania danych – obowiązek informacyjny	128
4.1.3. Test uzasadnionego interesu (LIA), jako narzędzie weryfikujące legalność przetwarzania danych	130
4.2. Obowiązki administratora vs podmiotu przetwarzającego.	
Szacowanie ryzyka i odpowiedzialność	131
4.2.1. Rodzaje zagrożeń wpływające na prawa i wolności podmiotów danych	133
4.2.2. Rejestrowanie czynności przetwarzania	135
4.2.3. Bezpieczeństwo przetwarzania	137
4.2.4. Ocena skutków dla ochrony danych (DPIA)	138
4.2.5. Przekazywanie danych do państw trzecich	141
4.3. Realizacja praw osób fizycznych na przykładzie kandydatów do pracy na gruncie RODO i AI Act	142

CZĘŚĆ III

Wdrożenie i dokumentacja. Aspekt praktyczny 147

ROZDZIAŁ 5

Plan wdrożenia agenta AI krok po kroku	148
5.1. Faza 1: Audyt strategiczny i uzasadnienie biznesowe wdrożenia agenta AI	149
5.1.1. Ocena potencjału i analiza luki rynkowej	149
5.1.2. Identyfikacja problemów operacyjnych	150
5.1.3. Gotowość firmy do wdrożenia Agentu AI	153
5.2. Faza 2. Planowanie projektu i założenia biznesowo-finansowe	155
5.2.1. Kryteria sukcesu PoC oraz zakres odpowiedzialności systemu	155
5.2.2. Role i odpowiedzialności	158
5.2.3. Założenia finansowe	160
5.3. Faza 3: Walidacja prawna – Weryfikacja zgodności z AI Act, RODO i Data Act	162
5.4. Faza 4: Proof of Concept (PoC) i MVP agenta AI	170
5.4.1. Zakres MVP	170
5.4.2. Główny przepływ PoC (<i>happy path</i>)	173
5.4.3. Architektura techniczna MVP (<i>high-level</i>)	175
5.4.4. Platforma HR i model danych	179
5.4.5. Generowanie feedbacku (copilot w ramach Agentu AI)	184

5.4.6. Walidacja jakości i korekta treści (<i>quality gate</i>)	187
5.4.7. Obsługa komunikacji e-mail – routing i eskalacja	190
5.5. Faza 5: Integracja i zarządzanie zmianą	195
5.5.1. Etapy wdrożenia zmiany	196
5.5.2. Komunikacja i rozwój kompetencji	199
5.6. Faza 6: Rozszerzenia produkcyjne i ścieżka ewolucji systemu	200
Zakończenie	204
Załączniki	207
DODATEK A	
Wzory i szablony dokumentacji	208
A.1. Przykładowa Polityka wdrożeniowa systemów AI w firmie	208
A.2. Wzór obowiązku informacyjnego RODO dla kandydatów do pracy (rekrutacja z wykorzystaniem systemu AI)	217
A.3. Ocena skutków przetwarzania danych osobowych (art. 35 RODO) – wzór kwestionariusza DPIA	220
A.4. Test uzasadnionego interesu (LIA) dla procesu rekrutacji, w którym wykorzystywany jest agent AI do przesyłania odpowiedzi kandydatom	230
A.5. Przykładowa instrukcja realizacji żądań podmiotów danych na gruncie RODO z prawem do uzyskania wyjaśnień na podstawie AI Act	235
A.6. Ocena poziomu ochrony danych osobowych w państwie trzecim i konieczności zastosowania dodatkowych środków bezpieczeństwa (TIA)	245
A.7. Ocena sposobów zabezpieczeń stosowanych przez podmiot przetwarzający	251
A.8. Analiza etycznych aspektów systemów AI	258
DODATEK B	
Narzędzia i zasoby	260
B.1. Słownik podstawowych pojęć prawnych i informatycznych	260
B.2. Lista kontrolna gotowości organizacji do wdrożenia systemu AI w MŚP	270
B.3. Plan komunikacji i szkoleń w procesie wdrażania systemu AI	274
B.4. Repozytorium kodu	277
Bibliografia	278
Spis rysunków i tabel	282
O Autorach	284