Audyt ochrony danych osobowych w praktyce. Przewodnik dla IOD + wzory do pobrania

Spis treści

Spis treści

O Autorach XV
Wykaz skrótów XVII
Wprowadzenie XXV

Rozdział I. Wprowadzenie do audytu i audytowania (*Tomasz Izydorczyk*) 1
1. Definicje i rozumienie pojęcia „audytu" 1
2. Istota i funkcje audytu w zapewnieniu zgodności z RODO 3
2.1. Audyt w art. 28 ust. 3 lit. h RODO 3
2.2. Audyt w art. 39 ust. 1 lit. b RODO 5
2.3. Audyt w art. 47 ust. 2 lit. j RODO 6

Rozdział II. Idea audytu w systemie ochrony danych osobowych – cel, wady i zalety (*Damian Bielecki*) 9
1. Cele audytu 9
2. Zalety audytu 10
2.1. Identyfikacja słabości i zagrożeń 10
2.2. Zapewnienie zgodności z regulacjami prawnymi 11
2.3. Ocena efektywności polityk i procedur 11
2.4. Szkolenia i edukacja personelu 12
2.5. Dokumentowanie zgodności 12
2.6. Pozyskanie argumentów przed spotkaniem z zarządem 13
2.7. Weryfikacja jakości usług świadczonych przez podmiot przetwarzający 13
2.8. Zwiększenie zaufania klientów i partnerów 14
2.9. Optymalizacji procesów biznesowych 15
3. Wady audytu 15
3.1. Kosztowność 15
3.2. Czasochłonność 16
3.3. Możliwość zakłóceń w działalności operacyjnej 16
3.4. Skupienie na zgodności, a nie na efektywności 17
3.5. Ryzyko powierzchowności/złudne wrażenie prawidłowości 17

3.6. Stres i opór pracowników 18
3.7. Ograniczona skuteczność w dynamicznych środowiskach 18
3.8. Ryzyko wykorzystywania wyników audytu przez organy nadzorcze 19
4. Wpływ audytu na inne obowiązki wynikające z RODO 19
4.1. Audyt jako punkt wyjścia 19
4.2. Zmapowanie danych i procesów 20
4.3. Efektywność procesów 20
4.4. Precyzyjne kierowanie pytań 20
5. Podsumowanie 20

Rozdział III. Audyt RODO a inne rodzaje audytów (*Agnieszka Gębicka/Piotr Nowicki – pkt 3, Beata Konieczna-Drzewiecka – pkt 1, Monika Sobczyk – pkt 2, Mariola Więckowska – pkt 4*) 23
1. Audyt zgodności z RODO 23
2. Audyt zgodności z normą ISO/IEC 27001 przeprowadzony przez IOD 27
2.1. Definicje 27
2.2. Kluczowe zasady i narzędzia 28
2.3. Cel audytu 28
2.4. Zakres audytu 29
2.5. Podstawa prawna i normatywna 29
2.6. Metody realizacji audytu 31
2.7. Charakterystyka normy ISO/IEC 27001 32
2.8. Planowanie audytu 33
2.9. Kryteria audytu 33
2.10. Zasoby i kompetencje audytora 34
2.11. Harmonogram audytu 35
2.12. Dokumentacja niezbędna do audytu 37
2.13. Przeprowadzenie audytu 37
2.13.1. Przegląd dokumentacji SZBI 37
2.13.2. Identyfikacja i ocena ryzyka 38
2.13.3. Analiza zabezpieczeń organizacyjnych i technicznych 40
2.13.4. Testy kontrolne 41
2.13.5. Analiza incydentów 44
2.13.6. Ocena zgodności i wykryte niezgodności 45
2.13.7. Raportowanie zgodności i niezgodności 46
2.13.8. Plan działań naprawczych 47
2.13.9. Prezentacja wyników audytu 48
2.13.10. Monitorowanie i przegląd działań naprawczych 51
2.13.11. Podsumowanie audytu – kluczowe wnioski 52
3. Audyt zgodności z wymaganiami NIS2 – rola inspektora ochrony danych 53
3.1. Uwagi wstępne 53

3.2. Etapy audytu zgodności z NIS2 – perspektywa inspektora ochrony danych 54
3.3. Przykłady z praktyki – teoria w kontekście realnych działań 56
3.4. Prosta checklista audytowa dla IOD – pytania na start 57
4. Audyt zgodności z wymaganiami rozporządzenia DORA z perspektywy IOD 58
4.1. Uwagi wstępne 58
4.2. Pięć filarów, na których opiera się DORA 58
4.3. Audyt zgodności z DORA 60
4.3.1. Plan audytu 60
4.3.2. Podejmowane działania audytowe 61
4.3.3. Połączenie i wpływ audytu DORA na zgodność z RODO 62
4.3.4. Podstawowe obszary audytu 62
4.3.5. Samoocena zgodności z wymogami DORA 63
4.3.6. Identyfikacja luk w procesach i systemach 63
4.3.7. Dokumenty i procedury podczas audytu DORA 64
4.3.8. Narzędzia i technologie wspomagające przygotowania do audytu DORA 65
4.3.9. Działania naprawcze w przypadku wykrycia niezgodności podczas audytu 66
4.3.10. Podsumowanie 66

Rozdział IV. Niezależność inspektora ochrony danych w audycie i kontroli
(*Agnieszka Gębicka/Piotr Nowicki – pkt 1 i 5, Beata Konieczna-Drzwiecka – pkt 2–4, Damian Bielecki – pkt 6*) 69
1. Pojęcie i rozumienie niezależności IOD 69
1.1. Podstawy prawne niezależności IOD 71
1.2. Najważniejsze zasady autonomii IOD 73
1.3. Niezależność IOD a formy jego zatrudnienia 87
2. Kontrola w administracji publicznej 94
2.1. Pojęcie kontroli 94
2.2. Rodzaje kontroli 96
2.3. Kontrola zewnętrzna nad administracją na przykładzie kontroli NIK 98
2.4. Kontrola wewnętrzna w jednostkach organizacyjnych administracji publicznej 101
3. Kontrola przetwarzania danych osobowych 102
3.1. Kontrola sprawowana przez Prezesa UODO 102
3.2. Kontrola sprawowana przez podmioty przetwarzające dane 104
3.3. Kontrola sprawowana przez osobę, której dane poddawane są przetwarzaniu 104
4. Audyt wewnętrzny w jednostkach organizacyjnych administracji publicznej a audyt IOD 105
5. Audyt IOD a audyt systemów zarządzania 115
5.1. Audyt IOD – obowiązek wynikający z przepisów RODO 115

5.2. Audyt ISO 27001 – systemowy i szerokozasięgowy 116
5.3. Audyt IOD a audyt ISO 27001 – różnice w praktyce 117
5.4. Audyt IOD – praktyka, nie formalność 117
6. Rola IOD w procesie *due diligence* 119
6.1. Proces *due diligence* 119
6.2. Znaczenie baz danych osobowych 119
6.3. Zadania IOD w procesie *due diligence* 119
6.4. Zakres analizy *due diligence* w kontekście baz danych 120
6.5. Konsekwencje dla IOD spółki objętej procesem *due diligence* 120

Rozdział V. Procedura audytu zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (*Beata Konieczna-Drzewiecka*) 123
1. Cel procedury 123
2. Adresaci procedury 124
3. Pojęcia audytowe 124
4. Poufność w audycie 125
5. Plan audytów, powołanie zespołu, dokumentacja 126
6. Czynności audytowe 128
6.1. Rozpoczęcie audytu 128
6.2. Trwanie audytu 130
6.3. Dokumentowanie ustaleń i wyników z audytu 131
6.4. Udział ekspertów wewnętrznych i zewnętrznych 133
7. Zakończenie audytu – decyzje poaudytowe 134
8. Wzory dokumentów 135
8.1. Wzór upoważnienia do przeprowadzenia audytu 135
8.2. Wzór oświadczenia o braku lub istnieniu okoliczności uzasadniających wyłączenie z udziału w audycie 136
8.3. Wzór protokołu oględzin 137
8.4. Wzór protokołu pobrania dokumentu/rzeczy 138
8.5. Wzór protokołu przyjęcia ustnych wyjaśnień/oświadczeń 138
8.6. Wzór upoważnienia dla eksperta 139

Rozdział VI. Audytowanie (*Damian Bielecki*) 141
1. Planowanie audytów 141
1.1. Roczne plany audytów 141
1.2. Audyty doraźne 142
2. Przygotowanie do audytów 142
2.1. Wywiad środowiskowy 143
2.2. Ankiety wstępne 143
2.2.1. Typowe pytania w ankietach wstępnych 144
2.2.2. Wyzwania związane z ankietami wstępnymi 144
3. Pierwsze spotkanie 144

3.1. Wyjaśnienie procesu audytu 145
3.2. Przyjmowanie założeń 145
3.3. Rozpisanie grafiku działań 146
3.4. Pełnomocnictwa 146
3.5. Ryzyka w audycie 147
4. Realizacja audytów 148
4.1. Audyt obszarów przetwarzania 148
4.2. Audyt zdalny 150
4.3. Rola audytora w procesie 151
4.4. Techniki zadawania pytań w trakcie audytu 151
4.5. Przegląd dokumentacji 152
4.5.1. Przegląd wzorów dokumentów 152
4.5.2. Metoda próbkowania 153
5. Dokumentowanie audytów 153
5.1. Notatki i nagrania z audytów 153
5.2. Ewidencjonowanie podjętych działań 154
5.3. Wzory raportów 155
6. Sprawozdanie z audytu 156
6.1. *Executive summary* 156
6.2. Zachowanie umiaru w raportowaniu ryzyk 156
7. Podsumowanie 157
8. Wzory dokumentów 158
8.1. Wzór ankiety przedaudytowej 158
8.2. Wzór grafiku audytu ochrony danych osobowych 160
8.3. Wzór raportu z audytu 161

Rozdział VII. Działania następcze (*Tomasz Izydorczyk – pkt 3–5, Monika Sobczyk – pkt 1–2 i 6*) 163
1. Dokumentowanie niezgodności 163
1.1. Znaczenie dokumentowania niezgodności 163
1.2. Najczęstsze błędy popełniane podczas dokumentowania niezgodności 165
2. Rekomendacje poaudytowe 167
3. Działania korekcyjne 169
4. Działania korygujące 171
5. Działania zapobiegawcze 172
6. Monitorowanie działań doskonalących 175
6.1. Rejestr niezgodności 175
6.2. Wskaźniki KRI a monitorowanie ryzyka 175
7. Wzory dokumentów 177
7.1. Wzór karty niezgodności/obserwacji 177
7.2. Wzór planu działań korygujących/zapobiegawczych 177

7.3. Wzór rejestru działań 178
7.4. Wzór rejestru niezgodności 178

Rozdział VIII. Specyfika audytów w różnych procesach (*Damian Bielecki – pkt 4 i 5, Agnieszka Gębicka/Piotr Nowicki – pkt 6, Beata Konieczna-Drzewiecka – pkt 3 i 7, Monika Sobczyk – pkt 8, Mariola Więckowska – pkt 1 i 2*) 179
1. Audytowanie środowiska informatycznego, w tym procesów i systemów IT 179
1.1. Historia audytu IT 179
1.2. Definicje 180
1.3. Proces zarządzania bezpieczeństwem systemów informatycznych 182
1.4. Dobre praktyki i normy ISO wspierające audyt procesów IT 183
1.5. Bezpieczeństwo przetwarzania danych z perspektywy wypełniania art. 32 RODO 183
1.5.1. Dobór zabezpieczeń 184
1.5.2. Procesy zarządzania bezpieczeństwem środowiska informatycznego 186
1.5.2.1. Zarządzanie konfiguracją 186
1.5.2.2. Zarządzanie zmianą 187
1.5.3. Zarządzanie ryzykiem środowiska informatycznego 188
1.5.3.1. Model zarządzania ryzykiem 188
1.5.3.2. Szacowanie ryzyka 189
2. Audytowanie systemów IT 191
2.1. Rodzaje audytów systemów IT 191
2.2. Normy, standardy i dobre praktyki dla audytu IT 191
2.3. Zakres audytowania 193
2.4. Audyt planów ciągłości działania i ich testów, zasady tworzenia i odtwarzania kopii zapasowych 193
2.5. Dobre praktyki w zakresie wykonania audytu systemów teleinformatycznych 195
2.6. Narzędzia wspomagające audyt 196
2.7. Wzór – przykładowa lista audytowa systemu teleinformatycznego 197
3. Audytowanie procesów kadrowych 204
3.1. Plan audytu 204
3.2. Cel audytu 205
3.3. Zakres audytu 205
3.4. Etapy audytu 206
3.4.1. Przygotowanie do audytu 206
3.4.2. Analiza dokumentacji 206
3.4.3. Analiza stanu faktycznego 207
3.4.3.1. Organizacja procesu rekrutacji 207
3.4.3.2. Organizacja zatrudnienia 208

3.4.3.3. Organizacja zmiany warunków zatrudnienia 210
3.4.3.4. Organizacja zakończenia zatrudnienia 213
3.4.4. Opracowanie sprawozdania z audytu 215
3.4.5. Działania poaudytowe 215
4. Audytowanie procesów sprzedaży i marketingu 216
4.1. Analiza danych osobowych 216
4.2. Pliki *cookies* i inne technologie śledzące 218
4.3. Obsługa klienta 219
4.3.1. Analiza naruszeń 219
4.3.2. Ograniczenia uprawnień 220
4.3.3. Klauzule informacyjne i świadomość personelu 220
4.3.4. Monitoring efektywności pracowników 221
4.3.5. Elementy do sprawdzenia w ramach audytu 222
4.4. Nabywanie leadów 223
4.4.1. Weryfikacja procesu pozyskiwania leadów 223
4.4.2. Zgody marketingowe 223
4.4.3. Zakup bazy danych 224
4.5. Współpraca partnerska 224
4.5.1. Współpraca z influencerami 224
4.5.2. Współpraca z partnerami 224
4.6. Jakość baz danych i leadów 225
5. Audytowanie mediów społecznościowych 226
6. Audyt zgodności z wymogami dotyczącymi ochrony dzieci w środowisku cyfrowym 227
7. Audytowanie rozwiązań chmurowych 241
7.1. Planowanie audytu rozwiązań chmurowych 241
7.2. Plan audytu rozwiązań chmurowych 243
7.3. Cel audytu rozwiązań chmurowych 243
7.4. Zakres audytu rozwiązań chmurowych 244
7.5. Etapy audytu rozwiązań chmurowych 244
7.5.1. Przygotowanie audytu 244
7.5.2. Analiza dokumentacji 244
7.5.3. Analiza stanu faktycznego 245
7.5.3.1. Weryfikacja usługi chmurowej 245
7.5.3.2. Przykładowe pytania audytowe i obszary do sprawdzenia 245
7.5.4. Opracowanie sprawozdania z audytu 247
7.5.5. Działania poaudytowe 247
8. Audyt w podmiocie leczniczym 247
8.1. Aktywa 247
8.2. Dokumenty 248

8.3. Przygotowanie planu audytu 249
8.3.1. Przygotowanie listy aktywów i dokumentacji 249
8.3.2. Osoby biorące udział w audycie 251
8.4. Działania poaudytowe 252
8.5. Podsumowanie 252
8.6. Wzory dokumentów 253
8.6.1. Wzór planu audytu w podmiocie leczniczym 253
8.6.2. Wzór harmonogramu audytu w podmiocie leczniczym 254
8.6.3. Wzór raportu audytu w podmiocie leczniczym 255

Rozdział IX. Audyt podmiotu przetwarzającego (*Agnieszka Gębicka/Piotr Nowicki – pkt 1–8, Monika Sobczyk – pkt 9*) 259
1. Wprowadzenie do tematyki realizacji audytu u podmiotu przetwarzającego 259
2. Podstawy prawne audytu u podmiotu przetwarzającego 261
3. Wymagania formalne w umowie powierzenia 262
4. Przykładowe zapisy w umowach powierzenia 270
5. Zawiadomienie procesora 273
6. Organizacja i przeprowadzanie audytu u procesora 274
7. Rekomendacje dla podmiotu przetwarzającego 284
8. Specyfika audytowania podmiotu przetwarzającego w sektorze publicznym 289
9. Specyfika audytowania podmiotu przetwarzającego w sektorze medycznym 293
9.1. Rodzaje podmiotów współpracujących z podmiotem medycznym 293
9.2. Zawarcie umowy powierzenia 294
9.3. Weryfikacja podmiotu przetwarzającego (PP) przez podmiot medyczny (PM) 296
9.4. Weryfikacja podmiotu przetwarzającego jako minimalizacja ryzyk 297
9.5. Wzory dokumentów 298
9.5.1. Wzór procedury weryfikacji dostawcy 298
9.5.2. Załącznik Nr 1 do procedury weryfikacji dostawców – ankieta RODO dla dostawcy przetwarzającego dane w chmurze 300
9.5.3. Załącznik Nr 2 do procedury weryfikacji dostawców – umowa powierzenia przetwarzania danych osobowych 302
9.5.4. Załącznik Nr 3 do procedury weryfikacji dostawców – klauzula informacyjna dla dostawcy 303
9.5.5. Załącznik Nr 4 do procedury weryfikacji dostawców – umowa o zachowaniu poufności 305

Rozdział X. Audyt a sztuczna inteligencja (*Tomasz Izydorczyk – pkt 1, Mariola Więckowska – pkt 2*) 307
1. Wykorzystanie AI w Audycie 307
1.1. Czynności związane z audytem, do których można wykorzystać AI 307
1.2. Systemy AI, które mogą wspierać audyt 309
1.3. Bezpieczeństwo użycia AI w procesie audytowania 309

1.4. Ryzyka związane z użyciem AI w procesie audytowania 310
1.5. Ryzyka dla obiektywizmu w procesie audytowania i przeciwdziałanie im .. 311
2. Audyt systemów AI 311
2.1. Zakres audytu algorytmicznego 311
2.2. Proces audytu 312
2.2.1. Karta modelu 312
2.2.2. Mapa systemu 314
2.2.3. Momenty i źródła stronniczości 320
2.2.4. Testowanie pod względem stronniczości 327
2.2.5. Audyt wykorzystujący inżynierię wsteczną (opcjonalnie) 329
2.3. Raport z audytu 329
2.4. Opinia EROD o przetwarzaniu danych osobowych w kontekście modeli AI . 330
2.4.1. Ocena anonimowości danych 330
2.4.2. Ocena prawnie usprawiedliwionego interesu 331
2.4.3. Dokumentacja – zasada rozliczalności (art. 5 ust. 2 RODO) 331
2.5. Norma ISO/IEC 23894:2023 „Technologia informacyjna – Sztuczna inteligencja – Wytyczne dotyczące zarządzania ryzykiem” 332
2.5.1. Uwagi wstępne 332
2.5.2. Ocena ryzyka dla systemu AI 332