

Vademecum Inspektora Ochrony Danych / M. Byczkowski, A. Dopart, M. Gruszczyński, M. Gumularz, T. Izydorczyk, W. Jakubowski, M. Kołodziej, Ł. Kołodziejczyk, P. Kozik, A. Sajewicz, P. Siewert, M. Soczko, M. Trajpacki, G. Wanio, T. Wacirz, M. Więckowska, P. Więckowski. – Stan prawny: grudzień 2019. – Warszawa, 2020

Spis treści

Wykaz skrótów	XVII
Wykaz literatury	XXI
O Autorach	XXIX
Wprowadzenie	XXXV
Rozdział I. Rola i znaczenie inspektora ochrony danych	1
1. Doświadczenia w wykonywaniu funkcji inspektora ochrony danych (<i>Maciej Byczkowski</i>)	1
1.1. Wprowadzenie	1
1.2. Rola i znaczenie funkcji inspektora ochrony danych	1
1.3. Praktyka związana z wyznaczaniem inspektora ochrony danych	3
1.3.1. Obowiązek wyznaczenia inspektora ochrony danych	3
1.3.2. Inspektor ochrony danych jako funkcja lub stanowisko	4
1.3.3. Zasady rekrutacji inspektora ochrony danych	5
1.3.4. Nadawanie inspektorowi ochrony danych odpowiednich uprawnień	6
1.3.5. Wyznaczanie zastępcy oraz powoływanie zespołu inspektora ochrony danych	6
1.3.6. Inspektor ochrony danych w grupach kapitałowych	7
1.3.7. Publikowanie danych kontaktowych inspektora ochrony danych i zawiadamianie o nich Prezesa Urzędu Ochrony Danych Osobowych	8
1.4. Praktyka związana z zapewnieniem wymaganego statusu inspektora ochrony danych	9
1.4.1. Włączanie inspektora ochrony danych we wszystkie sprawy dotyczące przetwarzania danych	9
1.4.2. Zapewnienie inspektorowi ochrony danych zasobów do realizacji zadań	10
1.4.3. Zapewnienie inspektorowi ochrony danych możliwości wykonywania zadań	11
1.4.4. Zapewnienie inspektorowi ochrony danych niezależności i odpowiedniej podległości	11
1.4.5. Zapewnienie osobom, których dane dotyczą kontaktu z inspektorem ochrony danych	12
1.5. Realizacja zadań przez inspektora ochrony danych	13
1.5.1. Zadania główne inspektora ochrony danych	13

1.5.2. Pozostałe zadania inspektora ochrony danych	16
1.5.2.1. Udział w prowadzeniu dokumentacji dotyczącej przetwarzania danych	16
1.5.2.2. Udział w postępowaniu dotyczącym naruszenia ochrony danych	18
1.5.2.3. Udział w ocenie skutków dla ochrony danych	20
1.5.2.4. Udział w szacowaniu ryzyka związanego z ochroną danych	22
1.5.2.5. Pełnienie funkcji punktu kontaktowego dla podmiotów danych	23
1.5.2.6. Pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych	24
1.5.2.7. Wykonywanie zadań z uwzględnieniem ryzyka związanego z przetwarzaniem danych	25
1.5.3. Rozliczanie się z wykonywania zadań przez inspektora ochrony danych	26
1.6. Podsumowanie	27

2. Podstawy prawne powołania inspektora ochrony danych

<i>(Maciej Kołodziej)</i>	28
2.1. Wprowadzenie	28
2.2. Obowiązujące regulacje odnoszące się do inspektora ochrony danych	30
2.3. Wyznaczenie inspektora ochrony danych na podstawie RODO	31
2.4. Wyznaczenie inspektora ochrony danych zgodnie z ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości	35
2.5. Zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu inspektora ochrony danych	36
2.6. Publikacja danych inspektora ochrony danych i jego zastępcy	36
2.7. Status inspektora ochrony danych	36
2.7.1. Status inspektora ochrony danych określony w przepisach RODO	36
2.7.2. Status inspektora ochrony danych określony w przepisach ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości	37
2.8. Zadania inspektora ochrony danych	37
2.8.1. Zadania inspektora ochrony danych w przepisach RODO	37
2.8.2. Zadania inspektora ochrony danych w przepisach ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości	38
2.9. Rozpoznane problemy związane z większą liczbą inspektorów ochrony danych	39
2.10. Inne zagadnienia dotyczące inspektorów ochrony danych	41
2.10.1. Umowa z zewnętrznym inspektorem ochrony danych (outsourcing)	41
2.10.2. Inspektor ochrony danych jako osoba świadcząca usługi w działalności gospodarczej	41
2.10.3. Ubezpieczenie odpowiedzialności zawodowej inspektora ochrony danych	42
2.11. Podsumowanie	42

3. Cechy dobrego inspektora ochrony danych (<i>Maciej Gruszczyński, Tomasz Wącirz</i>)	42
3.1. Wprowadzenie	42
3.2. Kompetencje inspektora ochrony danych	43
3.3. Źródła wiedzy potrzebnej do pełnienia funkcji inspektora ochrony danych	45
3.3.1. Wydawnictwa prasowe i publikacje książkowe	45
3.3.2. Serwisy internetowe	46
3.3.3. Stowarzyszenia i grupy branżowe	48
3.3.4. Szkolenia oraz studia kierunkowe	49
3.3.5. Źródła obowiązkowe i uzupełniające	50
3.4. Wiedza spoza zakresu ochrony danych osobowych, którą inspektor powinien posiadać	50
3.5. Funkcjonowanie inspektora ochrony danych w organizacji	51
3.5.1. Wiedza na temat organizacji	52
3.5.2. Kompetencje miękkie	53
3.5.3. Technologia w organizacji	54
3.5.4. Znajomość języków obcych i żargonu stosowanego u administratora	56
3.5.5. Inwentaryzacja zasobów organizacji	57
3.5.6. Budowanie świadomości pracowników administratora	58
3.5.7. Komunikacja z otoczeniem	61
3.6. Administrator danych osobowych a inspektor danych osobowych	65
3.6.1. Podział obowiązków między administratorem a inspektorem danych osobowych	65
3.6.2. Zadania inspektora ochrony danych	66
3.6.3. Fakultatywne zadania, w których inspektor ochrony danych może uczestniczyć	67
3.6.4. Błędy popełniane przez inspektorów ochrony danych	68
3.6.5. Rozliczalność inspektora danych osobowych	69
3.7. Zasoby umożliwiające inspektorowi ochrony danych prawidłową realizację zadań	70
3.8. Dodatkowe narzędzia wspierające pracę inspektora ochrony danych	71
3.9. Podsumowanie	72
 4. Organizacja wypełniania obowiązków dotyczących ochrony danych osobowych w grupie przedsiębiorstw (<i>Paweł Więckowski</i>)	 72
4.1. Wprowadzenie	72
4.2. Model operacyjny ochrony danych w grupie przedsiębiorstw	73
4.3. Struktura zarządzania ochroną danych	73
4.3.1. Funkcja inspektora ochrony danych w grupie przedsiębiorstw	73
4.3.2. Podstawowe role w procesie ochrony danych osobowych	75
4.3.3. Wspólne polityki, standardy i procedury ochrony danych osobowych	76
4.3.4. Polityka ochrony danych osobowych	77
4.3.5. Jednolity standard ochrony danych osobowych	79
4.3.5.1. Uniwersalne zasady ochrony danych osobowych	80

4.3.5.2. Działania wymagane w celu spełnienia zasad ochrony danych osobowych	83
4.3.5.3. Słownik kategorii osób, których dane dotyczą	86
4.3.5.4. Słownik poziomów wrażliwości kategorii danych osobowych	88
4.4. Standaryzacja	92
4.4.1. Wspólny rejestr czynności przetwarzania i ocen skutków dla ochrony danych	92
4.4.2. Centralne zarządzanie incydentami ochrony danych	93
4.4.3. Scentralizowany proces obsługi praw osób, których dane dotyczą	95
4.4.3.1. Wyjątki od procesu obsługi wniosków dotyczących praw osób	96
4.4.3.2. Kanały wpływu wniosków osób o wykonanie przysługujących im praw	96
4.4.3.3. Odbiór i walidacja wniosków	97
4.4.3.4. Wypełnianie wniosków	97
4.4.3.5. Udzielanie odpowiedzi na wnioski	97
4.5. Kompetencje i świadomość organizacji	98
4.6. Zgodne z prawem przekazywanie danych w grupie	100
4.7. Podsumowanie	101

5. Narzędzia wspierające pracę inspektora ochrony danych

(Łukasz Kołodziejczyk) **102**

5.1. Wprowadzenie	102
5.2. Kontekst organizacji i procesów przetwarzania danych osobowych	102
5.3. Oczekiwania i wymagania organizacji (funkcja celu)	103
5.4. Modele świadczenia usług	104
5.5. Kryteria wyboru narzędzi i wymagania funkcjonalne	106
5.5.1. Sposób pracy w organizacji	107
5.5.2. Sposób realizacji usługi	107
5.5.3. Koszty związane z wyborem oraz wdrożeniem wybranych narzędzi	108
5.5.4. Funkcje i funkcjonalność oferowane przez narzędzia	109
5.5.5. Wsparcie producenta i dokumentacja produktu	111
5.6. Opis wybranych rozwiązań	111
5.6.1. Oprogramowanie biurowe (arkusz kalkulacyjny i edytor tekstowy)	111
5.6.2. Strony WWW-systemy CMS i systemy ticketowe	112
5.6.3. Systemy zarządzania dokumentami (DMS)	114
5.6.4. Rozwiązania dedykowane	115
5.7. Podsumowanie	117

Rozdział II. Zmiany w prawie ochrony danych osobowych

119

1. Zakres zastosowania polskich i europejskich przepisów wchodzących w skład reformy ochrony danych osobowych

(Patrycja Kozik) **119**

1.1. Wprowadzenie	119
1.2. Materialny zakres stosowania RODO	119
1.3. Ustawa o ochronie danych osobowych	121
1.3.1. Zakres swobody regulacyjnej państw członkowskich	121
1.3.2. Zakres stosowania ustawy o ochronie danych osobowych	122

1.3.3. Przepisy zmieniające w ustawie o ochronie danych osobowych	123
1.4.. Przepisy sektorowe wdrażające RODO	126
1.4.1. Ustawa o zmianie niektórych ustaw w związku zapewnieniem stosowania RODO	126
1.4.2. Zmiany w zasadach przetwarzania danych w stosunkach pracy	127
1.5. Implementacja ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości	132
1.6. Podsumowanie	134

2. Wpływ RODO oraz ustawy wdrażającej RODO na prowadzenie Telemarketingu i działalności e-commerce - wybrane zagadnienia

(Anna Dopart, Grzegorz Wanio) **135**

2.1. Wprowadzenie	135
2.2. Zasady przetwarzania danych osobowych	136
2.2.1. Ustawa o świadczeniu usług drogą elektroniczną	136
2.2.2. Prawo telekomunikacyjne	141
2.3. Zbieranie danych osobowych - uproszczony obowiązek informacyjny	142
2.4. Wyrażenie zgody na podstawie przepisów o ochronie danych osobowych	145
2.5. Zakres przetwarzanych danych osobowych	151
2.6. Prowadzenie rejestru naruszeń danych osobowych	152
2.7. Kary za nieprzestrzeganie przepisów o ochronie danych osobowych	154
2.8. Podsumowanie	155

3. Transgraniczne przekazywanie danych osobowych - wskazówki praktyczne oraz perspektywa zmian związanych z brexitem

(Mariusz Trafacki) **155**

3.1. Wprowadzenie	155
3.1.1. Ogólny zarys problematyki transferu danych	155
3.1.2. Podstawowe pojęcia związane z przekazywaniem danych osobowych	156
3.2. Przekazywanie danych osobowych w ramach Europejskiego Obszaru Gospodarczego	158
3.3. Przekazywanie danych osobowych do państw trzecich	159
3.3.1. Ogólna zasada przekazywania danych osobowych do państw trzecich	159
3.3.2. Przekazywanie danych na podstawie decyzji Komisji Europejskiej w sprawie odpowiedniego poziomu ochrony danych osobowych	161
3.3.2.1. Decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony	161
3.3.2.2. Tarcza Prywatności	162
3.3.2.3. Decyzja Komisji Europejskiej w sprawie Kanady	163
3.3.3. Przekazywanie danych z zastrzeżeniem odpowiednich zabezpieczeń	164
3.3.3.1. Cechy mechanizmu odpowiednich zabezpieczeń	164
3.3.3.2. Prawnie wiążące i egzekwowalne instrumenty między organami lub podmiotami publicznymi	164
3.3.3.3. Wiążące reguły korporacyjne	165
3.3.3.4. Standardowe klauzule ochrony danych	166

3.3.3.5. Zatwierdzony kodeks postępowania oraz mechanizmy certyfikacji	167
3.3.3.6. Klauzule umowne oraz postanowienia uzgodnień administracyjnych	168
3.3.3.7. Wyjątki w szczególnych sytuacjach	168
3.4. Brexit i jego konsekwencje dla transferu danych do Wielkiej Brytanii	171
3.4.1. Obecne zasady przekazywania danych osobowych do Wielkiej Brytanii	171
3.4.2. Przekazywanie danych w przypadku twardego brexitu	172
3.4.3. Przekazywanie danych w przypadku zawarcia umowy o wystąpieniu Wielkiej Brytanii z Unii Europejskiej	173
3.5. Podsumowanie	173

Rozdział III. Praktyczne podejście do stosowania RODO **175**

1. Dane osobowe w dobie świata cyfrowego i Internetu (Maciej Kołodziej) **175**

1.1. Wprowadzenie	175
1.2. Pojęcie danych osobowych w kontekście świata nowych technologii	176
1.3. Dane osobowe pozyskane, przekazane i modyfikowane w procesach akwizycji, rejestracji, zmian profilowych i współpracy ze stronami	179
1.4. Dane uzyskane w procedurach importu ze źródeł zewnętrznych, w tym przewidzianego w przepisach przenoszenia danych osobowych	180
1.5. Dane przetwarzane w trakcie korzystania z usług przez podmioty danych i wywiązywania się z obowiązków przez administratora, w tym w zakresie władztwa i zobowiązań publicznych, realizacji praw lub umów	181
1.6. Dane wytworzone z inicjatywy podmiotu danych, na jego wniosek lub na jego rzecz	181
1.7. Dane powstałe w wyniku aktywności podmiotu danych w relacji z administratorem	182
1.8. Dane wytworzone przez administratora na rzecz podmiotu danych lub o podmiocie danych	182
1.9. Dane wywnioskowane lub wywiedzione przez administratora na temat podmiotu danych	183
1.10. Dane osobowe w cyberprzestrzeni	183
1.11. Podsumowanie	184

2. Sytuacje, kiedy administrator nie jest administratorem (Maciej Kołodziej) **185**

2.1. Wprowadzenie	185
2.2. Opis problemu w jednostkach administracji publicznej	185
2.3. Opis problemu w podmiotach biznesowych	187
2.4. Podział kompetencji przy stosowaniu RODO	187
2.5. Podsumowanie	188

3. Prowadzenie rejestru czynności przetwarzania danych osobowych i rejestru kategorii czynności przetwarzania, jako spełnienie obowiązku rozliczalności (Aleksandra Sajewicz) **189**

3.1. Wprowadzenie	189
-------------------	-----

3.2. Cel prowadzenia rejestrów	189
3.3. Podmioty zobowiązane do prowadzenia rejestrów	190
3.4. Prowadzenie rejestrów przez podmioty zatrudniające mniej niż 250 pracowników	191
3.5. Czynności przetwarzania, które powinny zostać ujęte w formie rejestru	193
3.6. Zawartość rejestru czynności przetwarzania	195
3.7. Zawartość rejestru kategorii czynności przetwarzania	198
3.8. Możliwość rozszerzenia katalogu informacji zawartych w rejestrach	201
3.9. Uchybienia w zakresie prowadzenia rejestrów stwierdzone przez organy nadzorcze	202
3.10. Forma prowadzenia rejestrów	204
3.11. Jawność rejestrów	205
3.12. Uwagi praktyczne	208
3.12.1. Analiza dokumentacji	208
3.12.2. Przygotowanie pytań do poszczególnych działów przedsiębiorstwa - ustalenie rzeczywistego zakresu przetwarzania danych w przedsiębiorstwie	209
3.12.3. Spotkania z właścicielami procesów przetwarzania danych oraz osobami mającymi kluczowy wpływ na zarządzanie przedsiębiorstwem	210
3.13. Konsekwencje naruszenia obowiązku prowadzenia rejestrów	210
3.14. Podsumowanie	211

4. Inspektor ochrony danych a ocena skutków dla ochrony danych (Mariola Więckowska) **212**

4.1. Wprowadzenie	212
4.2. Podejście oparte na ryzyku	212
4.3. Ochrona danych w fazie projektowania i domyślna ochrona danych	216
4.4. Ocena skutków dla ochrony danych	217
4.4.1. Założenia mechanizmu oceny skutków dla ochrony danych	217
4.4.2. Kryteria wskazujące, kiedy należy przeprowadzić ocenę skutków dla ochrony danych	218
4.4.3. Współadministrowanie i podpowierzenie przetwarzania danych a ocena skutków dla ochrony danych	219
4.4.4. Etapy oceny skutków dla ochrony danych	220
4.4.4.1. Etap 1 : wstępna ocena skutków dla ochrony danych - ogólna analiza ryzyka	221
4.4.4.2. Etap 2: analiza procesu lub jego zmiany oraz wpływu na prywatność	241
4.4.4.3. Etap 3: przygotowanie raportu końcowego wraz ze strategią postępowania z ryzykiem	258
4.4.4.4. Etap 4: monitoring wdrożenia	259
4.4.5. Korzyści z przeprowadzenia oceny skutków dla ochrony danych	260
4.4.6. Przykładowe formularze oceny skutków dla ochrony danych	260
4.5. Podsumowanie	267

5. Wykazywanie, że administrator regularnie testuje, mierzy i ocenia skuteczność środków technicznych i organizacyjnych

mających zapewnić bezpieczeństwo przetwarzania danych osobowych (<i>Maciej Kołodziej</i>)	268
5.1. Wprowadzenie	268
5.2. Metody weryfikacji jakości procesów	268
5.3. Wskazówki i wzorce przydatne w trakcie analizy jakości procesów	269
5.4. Prowadzenie dokumentacji przetwarzania danych osobowych	270
5.4.1. Dokumentacja ochrony danych osobowych w poprzednim stanie prawnym	271
5.4.2. Dokumenty obowiązkowe według RODO	271
5.5. Dokumentowanie stosowanych zabezpieczeń danych osobowych	272
5.6. Przeprowadzanie analizy ryzyka i odpowiednie jej dokumentowanie	273
5.7. Inne obszary, w których można wykazać staranność	274
5.8. Podsumowanie	277
 Rozdział IV. Umowy powierzenia przetwarzania danych	 279
 1. ABC umów powierzenia - przykłady zapisów, błędy i sposoby weryfikacji podmiotów przetwarzających (<i>Wojciech Jakubowski</i>)	 279
1.1. Wprowadzenie	279
1.2. Obowiązkowe elementy umowy powierzenia	280
1.3. Fakultatywne zapisy, które warto zamieścić w umowie powierzenia	282
1.4. Wybór odpowiedniego podmiotu przetwarzającego	284
1.5. Podsumowanie	286
 2. Nowe spojrzenie na konieczność zawarcia umowy powierzenia (<i>Marcin Soczko, Patryk Siewert</i>)	 287
2.1. Wprowadzenie	287
2.2. Interpretacja definicji umowy powierzenia	287
2.3. Zlecenie przetwarzania na podstawie umowy B2B	290
2.3.1. Przedsiębiorca podmiotem przetwarzającym	290
2.3.2. Przedsiębiorca jako osoba działająca z upoważnienia administratora	290
2.3.3. Ochrona danych jako wyznacznik konieczności zawierania umów powierzenia	291
2.4. Przetwarzanie danych przez zleceniobiorcę (na podstawie umowy cywilnoprawnej) - ocena konieczności zastosowania umowy powierzenia z punktu widzenia ochrony danych	292
2.5. Przetwarzanie danych przez telepracownika (na podstawie umowy o pracę) - ocena konieczności zastosowania zapisów umowuych, o których mowa w art. 28 RODO	293
2.6. Mniej typowe sytuacje przetwarzania danych we współpracy z innymi podmiotami	296
2.6.1. Hosting a kolokacja	296
2.6.2. Przetwarzanie na zlecenie podmiotów spoza Europejskiego Obszaru Gospodarczego, które są administratorami danych osób niebędących obywatelami Unii Europejskiej	297
2.6.3. Powierzenie przetwarzania danych nieosobowych (np. z numerami rejestracyjnymi pojazdów)	298

2.6.4. Powierzenie przetwarzania, gdy podmiot przetwarzający też jest administratorem	299
2.6.5. Przekazywanie służbowych danych kontaktowych w umowie	299
2.7. Podsumowanie	300

3. Przekazywanie danych wymagające zawarcia umowy powierzenia (<i>Tomasz Izydorczyk</i>)	300
3.1. Wprowadzenie	300
3.2. Definicja powierzenia przetwarzania danych osobowych	301
3.3. Różnice między powierzeniem a udostępnieniem	303
3.4. Sytuacje, gdy mimo powierzenia przetwarzania danych umowa nie jest potrzebna	304
3.5. Konsekwencje powierzenia i udostępnienia danych	304
3.5.1. Konsekwencje dla administratora (zleceniodawcy) w przypadku powierzenia przetwarzania	304
3.5.2. Konsekwencje dla procesora (zleceniobiorcy) w przypadku powierzenia przetwarzania	305
3.5.3. Konsekwencje dla zleceniodawcy (administratora) w przypadku udostępnienia danych zleceniobiorcy (drugiemu administratorowi)	305
3.5.4. Wspólne konsekwencje wynikające z powierzenia i udostępnienia	305
3.6. Test pomagający ustalić, czy dochodzi do powierzenia lub udostępnienia danych	305
3.7. Różnice między powierzeniem a współadministrowaniem	307
3.8. Zabezpieczenia dla procesora po zrealizowaniu umowy	307
3.9. Podsumowanie	307

Rozdział V. Naruszenie ochrony danych osobowych **309**

1. Naruszenie zasad ogólnych RODO jako źródło ryzyka naruszenia praw lub wolności (<i>Mirosław Gumularz</i>)	309
1.1. Wprowadzenie	309
1.2. Projektowanie ochrony danych a analiza ryzyka naruszenia praw lub wolności	310
1.3. Inne funkcje analizy ryzyka naruszenia praw lub wolności	311
1.4. Pojęcie ryzyka naruszenia praw lub wolności	311
1.5. Źródła naruszenia praw lub wolności	313
1.6. Podsumowanie	317

2. Zgłaszanie naruszenia ochrony danych osobowych (<i>Marcin Soczko, Patryk Siewert</i>)	317
2.1. Wprowadzenie	317
2.2. Konsekwencje nieprzestrzegania wymagań art. 33 RODO	318
2.3. Statystyki zgłoszeń w krajach wspólnoty europejskiej	320
2.4. Definicja naruszenia ochrony danych	321
2.5. Stwierdzenie wystąpienia naruszenia ochrony danych osobowych	322
2.6. Obowiązek zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych	323
2.6.1. Rozliczalność w ocenie prawdopodobieństwa wystąpienia ryzyka	

dla praw lub wolności osób fizycznych	324
2.6.2. Ocena występowania obowiązku zgłoszenia naruszenia ochrony danych	324
2.7. Podsumowanie	338
3. Środki minimalizacji ryzyka podczas przetwarzania danych osobowych (<i>Łukasz Kołodziejczyk</i>)	338
3.1. Wprowadzenie	338
3.2. Podstawowe prawa i wolności osób, których dane dotyczą, w kontekście operacji przetwarzania	339
3.3. Dobór odpowiednich technicznych i organizacyjnych środków bezpieczeństwa	340
3.4. Podsumowanie	347
Rozdział VI. Dział IT w otoczeniu inspektora ochrony danych	349
1. Komputer operatora danych a ochrona danych osobowych w systemie, cyberbezpieczeństwo, bezpieczeństwo informacji i tajemnica przedsiębiorstwa (<i>Maciej Kołodziej</i>)	349
1.1. Wprowadzenie	349
1.2. Wypracowane metody zarządzania bezpieczeństwem informacji przetwarzanych w systemach informatycznych	350
1.3. Aktualne wymogi dotyczące zarządzania procesem ochrony informacji	350
1.4. Współpraca inspektora ochrony danych z działem IT	353
1.5. Proces zautomatyzowanego przetwarzania danych osobowych	356
1.6. Rekomendowane środki zabezpieczające w procesach przetwarzania danych osobowych	358
1.7. Informacje cyfrowe i analogowe	359
1.8. Różnorodność i adekwatność środków ochrony w relacji do ryzyka przetwarzania	360
1.9. Komunikacja z pracownikami i współpracownikami	361
1.9.1. Poczta elektroniczna	361
1.9.2. Serwisy WWW	362
1.9.3. Dyski sieciowe	363
1.10. Wykorzystanie pseudonimizacji podczas przetwarzania danych	363
1.11. Kopie zapasowe i archiwalne	365
1.11.1. Wykonywanie kopii bezpieczeństwa - backup	366
1.11.2. Archiwizacja danych	366
1.11.3. Kompleksowe rozwiązania archiwizacyjne	367
1.12. Praktyka w zakresie ochrony stanowiska pracy	369
1.12.1. Stosowanie procedur AAA + w aplikacjach i systemach	369
1.12.1.1. Zasady właściwego nadzoru nad dostępem do danych	369
1.12.1.2. Weryfikacja tożsamości operatora danych i użytkownika systemu	371
1.12.1.3. Programy, aplikacje i narzędzia do przetwarzania danych	372
1.12.2. Aktywowanie wygaszaczy ekranu chronionych hasłem	373
1.12.3. Ustawienie limitów bezczynności dla sesji w aplikacjach	

i ich blokowanie	373
1.12.4. Obowiązkowe, automatyczne szyfrowanie nośników stałych i przenośnych	373
1.12.5. Ochrona przed szkodliwym oprogramowaniem	374
1.12.6. Korzystanie wyłącznie ze sprawdzonego oprogramowania	374
1.12.7. Zabezpieczenie systemów przed utratą zasilania	374
1.12.8. Szyfrowanie transmitowanych danych	375
1.12.9. Unikanie publicznych repozytoriów i dysków sieciowych	375
1.12.10. Kontrolowanie udostępnionych zasobów znajdujących się na własnych serwerach oraz usuwanie wykorzystanych danych z platform udostępniających informacje	375
1.13. Rozwiązania wspomagające bezpieczeństwo systemów informatycznych	376
1.13.1. Systemy DLP	376
1.13.2. Systemy MDM	376
1.13.3. Rozwiązania NAC	377
1.13.4. Prywatny sprzęt w systemach teleinformatycznych administratora (BYOD)	377
1.14. Zalecenia bezpieczeństwa dla systemów informatycznych	378
1.14.1. Hasła administracyjne w „kopercie”	378
1.14.2. Zakres usług i serwisów IT, w których przetwarzane są dane osobowe	379
1.14.3. Standard konfiguracji komputerowego stanowiska pracy	379
1.14.4. Inwentaryzacja serwerów	380
1.14.5. Rejestracja czasu zdarzeń	380
1.14.6. Serwerownia	381
1.14.7. Dostęp do sieci komputerowych i przekazywanie informacji	382
1.15. Podsumowanie	383

2. Inspektor ochrony danych a przetwarzanie z użyciem nowych technologii, w tym big data, bazy otwarte, sztuczna inteligencja oraz Internet rzeczy (Mariola Więckowska)	385
2.1. Wprowadzenie	385
2.2. Nowe technologie i ich wpływ na inspektora ochrony danych	386
2.2.1. Big data	386
2.2.1.1. Modele opisu big data	386
2.2.1.2. Działanie big data	387
2.2.1.3. Wykorzystanie big data	388
2.2.1.4. Zalety i wady big data	388
2.2.1.5. Inspektor ochrony danych w świecie big data	389
2.2.2. Bazy otwarte	390
2.2.2.1. Wykorzystywanie otwartych baz danych	390
2.2.2.2. Inspektor ochrony danych a bazy otwarte	391
2.2.3. Sztuczna inteligencja (AI) i uczenie maszynowe (ML)	392
2.3. Analiza big data	393
2.3.1. Elementy analizy big data	393
2.3.2. Typy danych	395
2.3.3. Wnioski z analizy big data	396

2.3.4. Zasady przetwarzania danych w kontekście skutków analizy big data dla podmiotów danych	397
2.3.4.1. Rzetelność	397
2.3.4.2. Podstawy prawne przetwarzania danych	398
2.3.4.3. Ograniczenie celu przetwarzania danych	398
2.3.4.4. Minimalizacja danych i ograniczenie przetwarzania	399
2.3.4.5. Prawidłowość danych	399
2.3.4.6. Prawa podmiotów danych	400
2.3.4.7. Zapewnienie bezpieczeństwa danych	400
2.3.4.8. Rozliczalność	401
2.3.5. Współpraca administratora z podmiotem przetwarzającym a analiza big data	402
2.3.6. Od big data do smart data	403
2.3.7. Narzędzia wspierające przetwarzanie danych w big data z wykorzystaniem sztucznej inteligencji i uczenia maszynowego	403
2.3.7.1. Anonimizacja danych	404
2.3.7.2. Obowiązek informacyjny	407
2.3.7.3. Ocena skutków dla ochrony danych	408
2.3.7.4. Ochrona danych w fazie projektowania i domyślna ochrona danych	408
2.3.7.5. Certyfikacja i znaki jakości	409
2.3.8. Etyczne podejście do przetwarzania danych	410
2.3.9. Przechowywanie danych w big data	411
2.3.10. Przejrzystość stosowanych algorytmów	412
2.4. Internet rzeczy	413
2.4.1. Znaczenie Internetu rzeczy we współczesnym świecie	413
2.4.2. Główne komponenty Internetu rzeczy	414
2.4.3. Internet rzeczy a przemysł	417
2.4.4. Zagrożenia płynące z Internetu rzeczy	417
2.4.5. Standardy i ustalone ramy stosowania Internetu rzeczy	419
2.5. Techniczne i organizacyjne środki bezpieczeństwa dla Internetu rzeczy i nowych technologii	420
2.5.1. Polityki bezpieczeństwa danych	421
2.5.2. Środki organizacyjne oraz ludzie i procesy	421
2.5.3. Środki techniczne	422
2.6. Podsumowanie	425