Ochrona danych osobowych od A do Z w 16 krokach

Spis treści

Spis treści

Wprowadzenie XVII
Wykaz skrótów XXI

Część I. Przewodnik od A do Z 1
Rozdział 1. Przygotowanie do kursu 9
1. Pięć motywatorów, aby zadbać o twój system ochrony danych 9
1.1. Katalog 9
1.2. Motywator 1: odpowiedzialność 10
1.3. Motywator 2: reputacja 11
1.4. Motywator 3: oszczędzanie czasu 12
1.5. Motywator 4: efektywność kosztowa 12
1.6. Motywator 5: szacunek dla osób fizycznych 13
1.7. Wsparcie od kierownictwa i interesariuszy 14
2. 10 różnic między firmą niedbającą o prywatność a twoimi celami 15
2.1. Uwagi wstępne 15
2.2. Różnica 1: cele przetwarzania danych 16
2.3. Różnica 2: zakres przetwarzanych danych osobowych 16
2.4. Różnica 3: weryfikacja i aktualizacja 17
2.5. Różnica 4: przechowywanie 18
2.6. Różnica 5: prawdopodobieństwo naruszenia bezpieczeństwa 19
2.7. Różnica 6: waga naruszenia 20
2.8. Różnica 7: prawa osób fizycznych 21
2.9. Różnica 8: formalna zgodność 22
2.10. Różnica 9: przejrzystość 23
2.11. Różnica 10: dowody 24
3. Dlaczego kontekst przetwarzania danych ma znaczenie? ... 25
3.1. Organizacja, którą będziesz obsługiwać 25

3.2. Znaczenie kontekstu organizacji 26
3.3. Gdzie zapisywać odpowiedzi? 27
3.4. Krótki opis działalności organizacji 28
3.5. Właściwe prawo i standardy 29
3.6. Jak uwzględnić lokalne i szczegółowe przepisy? 30
3.7. Szacowana liczba osób, których dane dotyczą 31
3.8. Lokalizacje, gdzie dane są przetwarzane 32
3.9. Jak będzie wyglądać twój projekt? 33
4. Cztery fazy – 16 kroków 34
4.1. Wprowadzenie 34
4.2. Faza 1: zidentyfikuj 35
4.3. Faza 2: oceń 36
4.4. Faza 3: wdrażaj 37
4.5. Faza 4: stosuj 37
5. Zacznij działać! 38
5.1. Wprowadzenie 38
5.2. Zespół ds. prywatności 39
5.3. Model zarządzania 40
5.4. Jak przygotować projekt? 42
5.5. Spotkanie inauguracyjne 43
5.6. Po spotkaniu inauguracyjnym 44
5.7. Wiadomość do wysłania rozmówcom (procesy) 45
5.8. Wiadomość do wysłania rozmówcom (zasoby) 46
5.9. Wiadomość do wysłania rozmówcom (ogólne obowiązki) 47
5.10. Twoja lista rzeczy do zrobienia (przygotuj się do startu) 48
Rozdział 2. Faza 1: Zidentyfikuj 49
1. Krok 1: Zidentyfikuj cele przetwarzania danych 49
1.1. Tryb działania 49
1.2. Procesy i przetwarzanie 50
1.3. Typowe procesy (administrator) 51
1.4. Typowe procesy (procesor) 52
1.5. Cele a procesy 53
1.6. Czyje są cele? 54
1.7. Których kwestionariuszy używać? 55
1.8. Operacje przetwarzania (kwestionariusz administratora) 56
1.9. Współadministratorzy (kwestionariusz administratora) . 57

1.10. Cele przetwarzania (kwestionariusz administratora) .. 58
1.11. Typowe cele (dodaj więcej szczegółów, jeśli to możliwe) 59
1.12. Administratorzy (kwestionariusz procesora) 60
1.13. Operacje i cele przetwarzania (kwestionariusz procesora) 61
1.14. Twoja lista rzeczy do zrobienia (krok 1) 61
2. Krok 2: Zidentyfikuj szczegóły przetwarzania danych 62
2.1. Kategorie podmiotów danych (kwestionariusz administratora) 62
2.2. Typowe kategorie podmiotów danych 63
2.3. Kategorie danych osobowych (kwestionariusz administratora) 64
2.4. Typowe kategorie „zwykłych" danych osobowych 65
2.5. Szczególne kategorie danych osobowych 66
2.6. Kategorie odbiorców (kwestionariusz administratora) 67
2.7. Typowe kategorie odbiorców 68
2.8. Przekazywanie danych poza Europejski Obszar Gospodarczy (kwestionariusz administratora) 69
2.9. Typowe przypadki przekazywania poza EOG 71
2.10. Planowane terminy usunięcia danych (kwestionariusz administratora) 72
2.11. Typowe terminy usunięcia danych 73
2.12. Ogólny opis środków bezpieczeństwa (zarówno kwestionariusze administratora, jak i procesora) 74
2.13. Przekazywanie danych poza EOG (kwestionariusz procesora) 75
2.14. Udzielanie gwarancji administratorom (kwestionariusz procesora) 76
2.15. Twoja lista rzeczy do zrobienia (krok 2) 76
3. Krok 3: Zidentyfikuj zasoby 77
3.1. Tryb działania 77
3.2. Jak pogrupować zidentyfikowane zasoby? 78
3.3. Lokalizacje i obszary 79
3.4. Typowe zasoby (lokalizacje i obszary) 80
3.5. Typowe zabezpieczenia (lokalizacje i obszary) 81
3.6. Sprzęt 83

3.7. Typowe zasoby (sprzęt) 84
3.8. Typowe zabezpieczenia (sprzęt) 85
3.9. Sieci i serwery 86
3.10. Typowe zasoby (sieci i serwery) 87
3.11. Typowe zabezpieczenia (sieci i serwery) 88
3.12. Strony internetowe 89
3.13. Typowe zasoby (strony internetowe) 90
3.14. Typowe zabezpieczenia (strony internetowe) 91
3.15. Oprogramowanie 92
3.16. Typowe zasoby (oprogramowanie) 93
3.17. Typowe zabezpieczenia (oprogramowanie) 94
3.18. Pliki elektroniczne (nieustrukturyzowane) 95
3.19. Typowe zasoby (pliki elektroniczne) 96
3.20. Typowe zabezpieczenia (pliki elektroniczne) 97
3.21. Wydrukowane dokumenty 98
3.22. Typowe zasoby (wydrukowane dokumenty) 99
3.23. Typowe zabezpieczenia (wydrukowane dokumenty) ... 100
3.24. Personel 101
3.25. Typowe zasoby (personel) 102
3.26. Typowe zabezpieczenia (personel) 103
3.27. Inne 104
3.28. Twoja lista rzeczy do zrobienia (krok 3) 106
4. Krok 4: Zidentyfikuj właścicieli procesów i zasobów 106
4.1. Właściciele procesów i zasobów 106
4.2. Właściciel procesu – typowe obowiązki 107
4.3. Właściciel zasobu – typowe obowiązki 108
4.4. Twoja lista rzeczy do zrobienia (krok 4) 110
Rozdział 3. Faza 2: oceń 111
1. Wstęp: faza oceny 111
1.1. Tryb działania 111
1.2. Rejestr czynności przetwarzania (kwestionariusze administratora) 112
1.3. Rejestr wszystkich kategorii czynności przetwarzania (kwestionariusze procesora) 113
2. Krok 5: Oceń procesy administratora 114
2.1. Cel 1: przetwarzaj dane tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach 114
2.1.1. Zasada ograniczenia celu (kwestionariusz administratora) 114

2.1.2. Zasada zgodności z prawem (kwestionariusz administratora) 115
2.1.3. Podstawy prawne udostępniania danych (kwestionariusz administratora) 116
2.2. Cel 2: przetwarzaj tylko te kategorie danych, które są niezbędne w twoim celu. Zasada minimalizacji danych (kwestionariusz administratora) 117
2.3. Cel 3: upewnij się, że dane osobowe są prawidłowe i aktualne. Zasada prawidłowości (kwestionariusz administratora) 118
2.4. Cel 4: usuwaj dane osobowe, które nie są już niezbędne w żadnym celu. Zasada ograniczenia przechowywania (kwestionariusz administratora) 119
2.5. Cel 5: chroń dane osobowe przed naruszeniem bezpieczeństwa 120
2.6. Cel 6: chroń osoby fizyczne przed naruszeniem ich praw 121
2.6.1. Obowiązek przeprowadzenia DPIA (kwestionariusz administratora) 121
2.6.2. Zagrożenia dla osób fizycznych (kwestionariusz administratora) 122
2.7. Cel 7: przygotuj się do obsługi żądań osób fizycznych . 124
2.8. Cel 8: spełnij wszystkie formalne wymogi prawne 125
2.8.1. Współadministratorzy (kwestionariusz administratora) 125
2.8.2. Typowe podatności (procesorzy) 126
2.8.3. Procesorzy zapewniający gwarancje zgodności (kwestionariusz administratora) 127
2.8.4. Procesorzy zobowiązali się przestrzegać wszystkich obowiązków z RODO (kwestionariusz administratora) 128
2.8.5. Zgodność z prawem przekazań poza EOG (kwestionariusz administratora) 129
2.9. Cel 9: podawaj osobom fizycznym wszystkie niezbędne informacje o ich prawach 130
2.9.1. Zasada przejrzystości (kwestionariusz administratora) 130
2.9.2. Podawanie wszystkich wymaganych informacji (kwestionariusz administratora) 131
2.9.3. Terminowe podawanie informacji (kwestionariusz administratora) 132

2.9.4. Cel 10: osiągnij rozliczalność – zdolność do wykazania zgodności 133
2.10. Twoja lista rzeczy do zrobienia (krok 5) 134
3. Krok 6: Oceń procesy procesora 136
3.1. Cel 1: przetwarzaj dane tylko w ramach umowy z administratorem 136
3.2. Cel 2: udziel administratorowi gwarancji ochrony danych. Udzielanie gwarancji administratorom (kwestionariusz procesora) 137
3.3. Cel 3: nie angażuj dalszego procesora bez zgody administratora i takich samych obowiązków 138
3.4. Cel 4: zapewnij poufność wszystkich osób upoważnionych do przetwarzania danych osobowych .. 139
3.5. Cel 5: chroń dane osobowe przed naruszeniem bezpieczeństwa 140
3.6. Cel 6: pomagaj administratorowi z żądaniami osób fizycznych 141
3.7. Cel 7: pomagaj administratorowi wypełniać inne obowiązki 142
3.8. Cel 8: wykaż administratorowi realizację obowiązków procesora 143
3.9. Twoja lista rzeczy do zrobienia (krok 6) 144
4. Krok 7: Oceń bezpieczeństwo informacji 145
4.1. Kryteria dla oceny bezpieczeństwa informacji 145
4.2. Tryb działania (ocena bezpieczeństwa informacji) 147
4.3. Przypadki wysokiego prawdopodobieństwa oraz ocena integralności i poufności 148
4.4. Lokalizacje i obszary 149
4.4.1. Typowe naruszenia bezpieczeństwa (lokalizacje i obszary) 149
4.4.2. Typowe podatności (lokalizacje i obszary) 150
4.5. Sprzęt 151
4.5.1.Typowe naruszenia bezpieczeństwa (sprzęt) 151
4.5.2. Typowe podatności (sprzęt) 152
4.6. Sieci i serwery 153
4.6.1. Typowe naruszenia bezpieczeństwa (sieci i serwery) 153
4.6.2. Typowe podatności (sieci i serwery) 154
4.7. Strony internetowe 155
4.7.1. Typowe naruszenia bezpieczeństwa (strony internetowe) 155

4.7.2. Typowe podatności (strony internetowe) 156
4.8. Oprogramowanie 157
4.8.1. Typowe naruszenia bezpieczeństwa (oprogramowanie) 157
4.8.2. Typowe podatności (oprogramowanie) 159
4.9. Pliki elektroniczne 160
4.9.1. Typowe naruszenia bezpieczeństwa (pliki elektroniczne) 160
4.9.2. Typowe podatności (pliki elektroniczne) 161
4.10. Wydrukowane dokumenty 162
4.10.1. Typowe naruszenia bezpieczeństwa (wydrukowane dokumenty) 162
4.10.2. Typowe podatności (wydrukowane dokumenty) 163
4.11. Personel 164
4.11.1. Typowe naruszenia bezpieczeństwa (personel) ... 164
4.11.2. Typowe podatności (personel) 165
4.12. Inne zasoby 166
4.13. Twoja lista rzeczy do zrobienia (krok 7) 167
5. Krok 8: Oceń ogólne obowiązki 168
5.1. Inspektor ochrony danych lub odpowiednik 168
5.1.1. Inspektor ochrony danych – wyznaczenie (kwestionariusz ogólnych obowiązków) 168
5.1.2. Inspektor ochrony danych – status (kwestionariusz ogólnych obowiązków) 169
5.1.3. Inspektor ochrony danych – zadania (kwestionariusz ogólnych obowiązków) 170
5.2. Zarządzanie naruszeniem i raportowanie 171
5.3. *Privacy by design* & *by default* 173
5.4. Prawa osób fizycznych 174
5.4.1. Prawo dostępu 174
5.4.2. Prawo do sprostowania 175
5.4.3. Prawo do usunięcia danych (do bycia zapomnianym) 176
5.4.4. Prawo do ograniczenia przetwarzania 177
5.4.5. Obowiązek powiadomienia o sprostowaniu, usunięciu lub o ograniczeniu przetwarzania 178
5.4.6. Prawo do przenoszenia danych 180
5.4.7. Prawo do sprzeciwu 181
5.4.8. Prawo, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu .. 182
5.5. Polityki i procedury 183
5.6. Obowiązki i świadomość pracowników 184

5.7. Podsumowanie dla kierownictwa i ocena ryzyka 185
5.8. Twoja lista rzeczy do zrobienia (krok 8) 187
Rozdział 4. Faza 3: wdrażaj 189
1. Krok 9: Modeluj procesy administratora 189
1.1. Wstęp: faza wdrożenia 189
1.2. Dostosuj zbieranie danych 190
1.3. Dostosuj zakres przetwarzania danych 191
1.4. Przygotuj klauzule informacyjne 192
1.5. Zaktualizuj umowy 193
1.6. Twoja lista rzeczy do zrobienia (krok 9) 195
2. Krok 10: Modeluj procesy procesora 196
2.1. Dostosuj zakres przetwarzania 196
2.2. Dostosuj komunikację z administratorem i podmiotami danych 197
2.3. Dostosuj umowy 198
2.4. Twoja lista rzeczy do zrobienia (krok 10) 199
3. Krok 11: Zarządzaj ryzykami bezpieczeństwa 200
3.1. Wstęp: zarządzanie ryzykami bezpieczeństwa 200
3.2. Ogólne cele, standardy i kontekst bezpieczeństwa 201
3.3. Przywództwo, role i obowiązki 202
3.4. Rejestr zasobów, analiza i zarządzanie ryzykiem 203
3.5. Zarządzanie zasobami, obsługa nośników i klasyfikacja informacji 205
3.6. Praca mobilna, praca z domu, prywatne urządzenia i wykorzystanie w celach prywatnych 206
3.7. Zarządzanie upoważnieniami i kontrolą dostępu 207
3.8. Bezpieczeństwo fizyczne i środowiskowe 208
3.9. Rejestrowanie zdarzeń oraz monitorowanie podatności i wykorzystania 210
3.10. Szyfrowanie 211
3.11. Relacje z dostawcami 212
3.12. Bezpieczeństwo sieci i przesyłanie informacji 213
3.13. Oprogramowanie – zabezpieczenia i zarządzanie podatnościami 215
3.14. Rekrutacja, zatrudnienie, zakończenie zatrudnienia i obowiązki użytkownika końcowego 216
3.15. Zarządzanie projektami, wyjątki i nietypowe zasoby ... 217
3.16. Zarządzanie naruszeniami 218
3.17. Ciągłość działania i odzyskiwanie po awarii 220

3.18. Przeglądy i ocena skuteczności 221
3.19. Twoja lista rzeczy do zrobienia (krok 11) 222
4. Krok 12: Przestrzegaj ogólnych obowiązków 225
4.1. Inspektor ochrony danych lub odpowiednik 225
4.2. Zarządzanie naruszeniem i raportowanie 226
4.3. *Privacy by design* 228
4.4. Prawa osób fizycznych 229
4.5. Obowiązek konsultacji z organem nadzorczym 230
4.6. Twoja lista rzeczy do zrobienia (krok 12) 231
Rozdział 5. Faza 4: stosuj 233
1. Krok 13: Przygotuj ogólne polityki 233
1.1. Wstęp: faza stosowania 233
1.2. Dlaczego ogólne polityki mają być użyteczne? 234
1.3. Jakie aspekty powinny obejmować polityki? 235
1.4. Jak przygotować ogólne polityki? 236
1.5. Relacja ze standardowymi procedurami postępowania (SOP) 237
1.6. Twoja lista rzeczy do zrobienia (krok 13) 238
2. Krok 14: Przygotuj procedury (SOP) 239
2.1. Ogólna SOP 239
2.2. Standardowe procedury operacyjne dla procesów administratora 241
2.3. Standardowe procedury operacyjne dla procesów procesora 242
2.4. Standardowe procedury operacyjne dla zasobów 243
2.5. Twoja lista rzeczy do zrobienia (krok 14) 244
3. Krok 15: Przyjmij, opublikuj i przeszkol 245
3.1. Przyjmij dokumentację ochrony danych 245
3.2. Opublikuj dokumentację ochrony danych 246
3.3. Przeszkol pracowników i współpracowników 248
3.4. Twoja lista rzeczy do zrobienia (krok 15) 249
4. Krok 16: Egzekwuj, utrzymuj i rewiduj 249
4.1. Egzekwuj wewnętrzne obowiązki 249
4.2. Utrzymaj zgodność i aktualność twojego systemu 251
4.3. Regularnie rewiduj i ulepszaj twój system ochrony danych 252
4.4. Twoja lista rzeczy do zrobienia (krok 16) 253
Rozdział 6. Podsumowanie 254

Część II. Szablony 257
Rozdział 1. Rozwiązania dla zgodności z prawem ochrony danych osobowych (GC szablony – część 1) 261
1. Wprowadzenie 261
2. System ochrony danych osobowych – projekt wdrożenia i utrzymania 262
3. Struktura dokumentu, zakres i kryteria 263
4. Ogólne informacje 263
5. Przypadki wysokiego ryzyka 265
6. Waga zagrożeń – perspektywa procesów 266
7. Prawdopodobieństwo naruszeń – perspektywa zasobów przetwarzających dane osobowe 266
8. Rekomendacje 267
9. Podsumowanie dla kierownictwa 268
9.1. Przegląd wyników 268
9.2. Zidentyfikowane przypadki wysokiego ryzyka 268
9.3. Identyfikacja i ocena 268
9.3.1. Kwestionariusze administratora 268
9.4. Kwestionariusze procesora – archiwizacja 272
9.5. Kwestionariusze właściciela zasobu 274
9.5.1. Lokalizacje i obszary 274
9.5.2. Sprzęt 275
9.5.3. Sieci i serwery 276
9.5.4. Strony internetowe 276
9.5.5. Oprogramowanie 277
9.5.6. Pliki elektroniczne 277
9.5.7. Wydrukowane dokumenty 278
9.5.8. Personel 279
10. Kwestionariusze ogólnych obowiązków 279
Rozdział 2. Rozwiązania dla zgodności z prawem ochrony danych osobowych – modelowanie i stosowanie (GC szablony – część 2) 283
1. Wprowadzenie 283
2. System ochrony danych osobowych – projekt wdrożenia i utrzymania 283
3. Krok 9: modeluj procesy administratora 285
3.1. Dostosuj zbieranie danych 285
3.2. Zadania 285
3.3. Szablon klauzuli zgody 286
4. Dostosuj zakres przetwarzania danych 286

5. Przygotuj klauzule informacyjne 287
5.1. Uwagi ogólne 287
5.2. Zadania 288
5.3. Lista kontrolna, aby upewnić się, że klauzula informacyjna zawiera wszystkie wymagane informacje .. 288
5.4. Skrócony wzór klauzuli 292
6. Zaktualizuj umowy 292
6.1. Uwagi ogólne 292
6.2. Zadania 294
6.3. Szablon umowy powierzenia przetwarzania 295
6.4. Szablon umowy administrator-administrator w celu przekazywania danych poza EOG 296
7. Krok 10: modeluj procesy procesora 296
7.1. Dostosuj zakres przetwarzania 296
7.2. Dostosuj komunikację z administratorem i podmiotami danych 297
7.3. Dostosuj umowy 298
7.4. Odpowiednie bezpieczeństwo przetwarzania (art. 28 ust. 3 lit. c RODO) 299
8. Krok 11: zarządzaj ryzykami bezpieczeństwa 299
8.1. Wprowadzenie 299
8.2. Ogólne cele, standardy i kontekst bezpieczeństwa 300
8.3. Przywództwo, role i obowiązki 300
8.4. Rejestr zasobów, analiza i zarządzanie ryzykiem 301
8.5. Zarządzanie zasobami, obsługa nośników i klasyfikacja informacji 302
8.6. Praca mobilna, praca z domu, prywatne urządzenia i wykorzystanie w celach prywatnych 303
8.7. Zarządzanie uprawnieniami i kontrolą dostępu 304
8.8. Bezpieczeństwo fizyczne i środowiskowe 304
8.9. Rejestrowanie zdarzeń oraz monitorowanie podatności i wykorzystania 305
8.10. Szyfrowanie 306
8.11. Relacje z dostawcami 307
8.12. Bezpieczeństwo sieci i przesyłanie informacji 308
8.13. Oprogramowanie – zabezpieczenia i zarządzanie podatnościami 308
8.14. Rekrutacja, zatrudnienie, zakończenie zatrudnienia i obowiązki użytkownika końcowego 309

8.15. Zarządzanie projektami, wyjątki i nietypowe zasoby ... 310
8.16. Zarządzanie naruszeniami ... 312
8.17. Ciągłość działania i odzyskiwanie po awarii ... 312
8.18. Przeglądy i ocena skuteczności ... 313
9. Krok 12: przestrzegaj ogólnych obowiązków ... 314
9.1. Inspektor ochrony danych lub odpowiednik ... 314
9.2. Zarządzanie naruszeniem i raportowanie ... 315
9.3. *Privacy by design* ... 317
9.4. Prawa osób fizycznych ... 318
9.5. Obowiązek konsultacji z organem nadzorczym ... 319
10. Krok 13: przygotuj ogólne polityki ... 319
11. Krok 14: przygotuj procedury (SOP) ... 321
12. Krok 15: przyjmij, opublikuj i przeszkol ... 322
12.1. Formalne przyjęcie dokumentacji ochrony danych ... 322
12.2. Publikacja dokumentacji ochrony danych ... 323
12.3. Szkolenie personelu ... 323
13. Krok 16: egzekwuj, utrzymuj i rewiduj ... 323
13.1. Regularne przeglądy i plan monitorowania ... 323
13.2. Karta budowania świadomości ... 324
13.3. Konsultacje z kierownictwem ... 324

Część III. Rozwiązania dla zgodności z prawem ochrony danych osobowych – GC szablony – przykład T&S ... 325
Rozdział 1. Uwagi ogólne ... 327
1. System ochrony danych osobowych – projekt wdrożenia i utrzymania ... 328
2. Struktura dokumentu, zakres i kryteria ... 330
2.1. Co zawiera część 1? ... 330
2.2. Ogólne informacje ... 330
2.3. Przypadki wysokiego ryzyka ... 332
2.4. Waga zagrożeń – perspektywa procesów ... 333
2.5. Prawdopodobieństwo naruszeń – perspektywa zasobów przetwarzających dane osobowe ... 333
2.6. Rekomendacje ... 334
Rozdział 2. Podsumowanie dla kierownictwa ... 335
1. Przegląd wyników ... 335
1.1. Procesy administratora ... 335
1.2. Procesy podmiotu przetwarzającego ... 336
1.3. Ogólne obowiązki ... 336

1.4. Bezpieczeństwo informacji 337
2. Zidentyfikowane przypadki wysokiego ryzyka 338
Rozdział 3. Identyfikacja i ocena 341
1. Kwestionariusze administratora 341
1.1. Rekrutacja 341
1.2. Pracownicy i współpracownicy 349
1.3. Księgowość i sprawozdawczość finansowa 357
1.4. Konkursy 364
1.5. Programy lojalnościowe 369
1.6. Wysyłki marketingowe i newsletter 375
1.7. Organizowanie wydarzeń 381
1.8. Reklamy i publikacje marketingowe 387
1.9. Potencjalni klienci (ofertowanie i sprzedaż) 392
1.10. Klienci (części samochodowe) 398
1.11. Klienci (naprawy samochodów) 404
1.12. Kontrahenci i dostawcy 410
1.13. Obsługa skarg i reklamacji 417
1.14. Obsługa prawna, windykacja i postępowania sądowe oraz administracyjne 423
1.15. Kontrola dostępu i monitoring wizyjny 429
1.16. Zarządzanie flotą i logistyka 435
2. Kwestionariusze procesora 441
2.1. Podwykonawstwo 441
2.2. Śledzenie pojazdów 445
3. Kwestionariusze właściciela zasobu 448
3.1. Lokalizacje i obszary 448
3.2. Sprzęt 451
3.3. Sieci i serwery 454
3.4. Strony internetowe 456
3.5. Oprogramowanie 457
3.6. Pliki elektroniczne 459
3.7. Wydrukowane dokumenty 461
3.8. Personel 463
4. Kwestionariusz ogólnych obowiązków 465

Indeks rzeczowy 471