

Spis treści

Wykaz skrótów	IX
Wprowadzenie	XI
Rozdział I. Opis metodyki przeprowadzenia kontroli zgodności z RODO	1
1. Uwagi ogólne	1
2. Ogólny zakres prac projektowych	2
3. Działy organizacji, które będą objęte projektem	5
4. Osoby, które będą uczestniczyły w realizacji projektu, reprezentując poszczególne obszary	6
5. Wyznaczenie project managera i koordynatora projektu	8
6. Analiza czy organizacja jest w stanie przeprowadzić kontrolę w ramach własnych zasobów	11
7. Ogólny harmonogram projektu	12
8. Techniczne zasady realizacji projektu	18
9. Budżet projektu	20
10. Odpowiednie wsparcie kierownictwa firmy	21
11. Inwentaryzacja zasobów zawierających dane osobowe	22
11.1. Zakres inwentaryzacji	22
11.2. Pozyskanie i weryfikacja dokumentacji wewnętrznej	24
11.3. Formularz inwentaryzacyjny	26
11.4. Weryfikacja zgodności przetwarzania danych osobowych z prawem	28
11.5. Procedury RODO – obowiązek wprowadzenia odpowiedniej dokumentacji ochrony danych osobowych	33
Rozdział II. Polityka RODO	37
1. Zawartość Polityki RODO	37
2. Efektywne ustalenie struktury osobowej odpowiedzialnej za poszczególne obowiązki RODO	38
3. Księga klauzul	39
4. Funkcje IOD i specjalisty RODO	40

5. Upoważnienie do przetwarzania danych osobowych oraz zobowiązanie osób do zachowania w tajemnicy	41
6. Przykładowy wzór Polityki RODO	42
Rozdział III. Procedura przetwarzania danych osobowych w organizacji	51
1. Zakres procedury przetwarzania danych osobowych	51
2. Dane osobowe osób fizycznych prowadzących działalność gospodarczą	52
3. Zasada zgodności z prawem, czyli legalność przetwarzania danych osobowych .	53
4. Zgoda i prawnie uzasadniony interes administratora jako podstawy prawne przetwarzania	54
5. Zgoda jako wyraźne działanie potwierdzające	54
6. Przykładowa procedura RODO dotycząca przetwarzania danych osobowych	55
Rozdział IV. Procedura ochrony danych osobowych przetwarzanych przez osoby upoważnione	69
1. Zakres procedury ochrony danych osobowych przetwarzanych przez osoby upoważnione	69
2. Upoważnienie do przetwarzania danych osobowych	70
3. Udostępnianie danych osobowych	72
4. Bezpieczne przechowywanie dokumentów w formie papierowej, zasada „czystego biurka”	73
5. Bezpieczne niszczenie dokumentów zawierających dane osobowe	74
6. Drukowanie danych osobowych na urządzeniach wspólnych	75
7. Mobilne nośniki danych osobowych	75
8. Nadawanie uprawnień do systemów informatycznych	76
9. Nadawanie loginów	77
10. Zakaz używania służbowego sprzętu w miejscach publicznych	77
11. Dostęp zdalny pracowników	77
12. Instrukcja zarządzania zmianą w systemach informatycznych	78
13. Poczta elektroniczna	79
14. Procedura zarządzania ciągłością działania	80
15. Kopie zapasowe	80
16. Procedura bezpieczeństwa teleinformatycznego	81
17. Wykorzystanie prywatnego sprzętu pracowników do celów służbowych w ramach zarządzania ciągłością działania	81
18. Przykładowa procedura dotycząca ochrony danych osobowych	82
Rozdział V. Procedura realizacji praw osób, których dane dotyczą	95
1. Zakres procedury	95
2. Odmowa realizacji wniosku	96
3. Tryb rozpatrywania wniosków o prawa RODO	97
4. Uprzednie poinformowanie o planowanym uchyleniu ograniczenia przetwarzania	98

5. Formularz wniosku o prawa RODO	99
6. Ścieżki składania wniosków o prawa RODO	99
7. Weryfikacja tożsamości osób składających wnioski	100
8. Przykładowa procedura dotycząca realizacji praw osób, których dane dotyczą ...	101
Rozdział VI. Procedura RODO dotycząca przeprowadzania oceny skutków dla ochrony danych	111
1. Zakres procedury	111
2. Ocena ryzyka dla ochrony danych	111
3. Metodyki przeprowadzania oceny skutków dla ochrony danych	113
4. Przykładowa procedura oceny skutków dla ochrony danych	114
Rozdział VII. Procedura zarządzania incydentami bezpieczeństwa danych osobowych	135
1. Zakres procedury zarządzania incydentami bezpieczeństwa danych osobowych	135
2. Postępowanie w razie zaistnienia incydentu bezpieczeństwa danych osobowych	135
3. Obowiązek poinformowania o incydencie PUODO oraz osób, których dane dotyczą	136
4. Inne metodyki	137
5. Rejestr incydentów bezpieczeństwa	137
6. Przykładowa procedura	137
Rozdział VIII. Instrukcja pełnienia funkcji IOD lub Specjalisty RODO oraz prowadzenia rejestrów czynności przetwarzania danych osobowych	155
1. Zakres instrukcji	155
2. Obowiązek powołania IOD	156
3. Wybór IOD	156
4. Obowiązek zgłoszenia IOD	158
5. Rejestry czynności przetwarzania	158
6. Przykładowa instrukcja pełnienia funkcji IOD i specjalisty RODO	159