

*Ochrona danych osobowych : ocena ryzyka i skutków :
metody i praktyczne przykłady*

redakcja Mirosław Gumularz, Tomasz Izydorczyk

SPIS TREŚCI

Wykaz skrótów | str. 9

Część 1

Pojęcie ryzyka naruszenia praw lub wolności

Rozdział 1. Wstęp – pojęcie ryzyka naruszenia praw lub wolności | str. 13

1. Przypadki oceny ryzyka w RODO – informacje ogólne | str. 13

Przepisy dotyczące oceny ryzyka | str. 13

A. Ogólny wymóg monitorowania ryzyka dla praw lub wolności (art. 24 ust. 1 RODO) | str. 14

B. Ocena ryzyka w fazie projektowania (art. 25 ust. 1 i 2 RODO) | str. 14

C. Ocena ryzyka pod kątem obowiązku prowadzenia rejestru czynności (art. 30 ust. 5 RODO) | str. 18

D. Ocena ryzyka w ramach oceny środków służących bezpieczeństwu (art. 32 ust. 1 RODO) | str. 18

E. Ocena ryzyka w ramach oceny incydentów bezpieczeństwa danych osobowych w kontekście obowiązku zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 ust. 1 RODO) | str. 22

F. Ocena ryzyka w ramach weryfikacji potrzeby zawiadamiania osoby, której dane są przetwarzane, w związku z incydem bezpieczeństwa (art. 34 ust. 1 RODO) | str. 24

G. Ocena ryzyka w ramach oceny skutków dla ochrony danych osobowych (art. 35 ust. 1 RODO)	str. 27
H. Ocena ryzyka dokonywana w ramach uprzednich konsultacji (art. 36 RODO)	str. 30
I. Ocena ryzyka dokonywana w kontekście sposobu realizacji zadań IOD (art. 39 ust. 2 RODO)	str. 31
J. Ocena ryzyka w kontekście transferu danych poza EOG	str. 33
K. Obowiązek informacyjny dotyczący ryzyka w kontekście transferu danych poza EOG	str. 34
L. Problem oceny ryzyka dla praw lub wolności w kontekście zadań organu nadzorczego (art. 57 ust. 1 lit. b RODO)	str. 35
M. Ocena ryzyka a zadania EROD (art. 64 ust. 1 lit. a)	str. 36
Szczególne przypadki oceny ryzyka	str. 36
N. Ocena ryzyka w kontekście stosowania RODO	str. 36
O. Ocena procesora (podmiotu przetwarzającego)	str. 37
P. Przetwarzanie danych osobowych w celach wskazanych w treści art. 89 ust. 1 RODO	str. 38
Q. Uzasadniony interes	str. 39
R. Zmiana celu przetwarzania danych	str. 40
2. Ramy regulacyjne oceny ryzyka – wstępne wnioski	str. 41
3. Jak rozumieć samo ryzyko?	str. 45
4. Problem identyfikacji przyczyn (źródeł) ryzyka	str. 46
Przyczyny ryzyka potencjalnego	str. 46
Przyczyny ryzyka zaistniałego	str. 48
Przyczyny ryzyka brane pod uwagę przez inspektora ochrony danych	str. 48
5. Jak należy rozumieć prawa lub wolności osób, których dane dotyczą, w kontekście oceny ryzyka?	str. 49
6. Jaki jest cel i uzasadnienie wprowadzenia regulacji opartej na risk based approach?	str. 51
7. Czym jest ryzyko naruszenia praw lub wolności osób, których dane dotyczą?	str. 52

8. Wymogi i „metawymogi” | str. 54

9. Czy naruszenie wymogu oceny ryzyka stanowi przetwarzanie niezgodne z prawem w rozumieniu RODO? | str. 56

10. Czy można uzyskać dostęp do dokumentacji oceny ryzyka w ramach dostępu do informacji publicznej? | str. 57

11. Elementy tła oceny ryzyka | str. 58

Ogólne (wspólne) elementy tła oceny ryzyka | str. 59

12. Co to jest systematyczny opis operacji przetwarzania danych osobowych? | str. 61

Rozdział 2. Źródło ryzyka naruszenia praw lub wolności | str. 66

1. Co może być źródłem ryzyka naruszenia praw lub wolności? | str. 66

2. Jak identyfikować zagrożenia? Jakie znaczenie ma zidentyfikowanie operacji na danych? | str. 67

3. Identyfikacja zagrożeń (źródeł ryzyka) metody | str. 68

4. Przykłady zagrożeń – identyfikacja w ramach naruszeń poszczególnych wymogów | str. 71

5. Przykłady zagrożeń – identyfikacja dla typowych procesów przetwarzania danych | str. 79

Rozdział 3. Szacowanie ryzyka naruszenia praw lub wolności | str. 82

1. Poziom ryzyka naruszenia praw lub wolności jako kombinacja dwóch elementów: prawdopodobieństwa wystąpienia zagrożenia i wagi tego zagrożenia | str. 82

Źródło czy skutek? | str. 82

Waga źródła ryzyka czy jego negatywnych skutków? | str. 83

Jedno zagrożenie – wiele negatywnych skutków. Jaka ocenić parametr wagi ryzyka? | str. 84

Prawdopodobieństwo wystąpienia zagrożenia czy wystąpienia jego skutków? | str. 85

Wiele zagrożeń – jedno ryzyko? | str. 86

Punkt odniesienia szacowania ryzyka. Proces? Operacja? Zagrożenie? | str. 89

2. Waga ryzyka naruszenia praw lub wolności | str. 89

3. Prawdopodobieństwo ryzyka | str. 90

Szacowanie prawdopodobieństwa ryzyka – różne podejścia | str. 90

Czynniki wystąpienia zagrożenia | str. 94

Czy można mówić o ryzyku, kiedy jego wystąpienie jest mało prawdopodobne? | str. 94

Ekspozycja ryzyka a wpływ na prawdopodobieństwo wystąpienia zagrożenia | str. 95

4. Podejście zagregowane czy cząstkowe – przykłady z metodyk | str. 95

5. Poziom ryzyka naruszenia praw lub wolności | str. 98

6. Postępowanie z ryzykiem na określonym poziomie | str. 101

Obszar niepewności | str. 101

Możliwe podejścia | str. 102

Rozdział 4. Wdrożenie środków technicznych lub organizacyjnych (zabezpieczeń) | str. 104

1. Poziom ryzyka a wdrożenie środków jego redukcji | str. 104

2. Wątpliwości wynikające z RODO | str. 105

3. Adekwatna reakcja | str. 105

4. Stan wiedzy i koszt wdrożenia | str. 106

5. ENISA – przykład innego podejścia | str. 106

6. Uwzględnienie obecnych środków i planowanie nowych | str. 107

7. Środki systemowe i zasada privacy by design | str. 108

Rozdział 5. Ocena skutków i uprzednie konsultacje | str. 114

1. Ocena skutków dla ochrony danych i uprzednie konsultacje | str. 114

2. Kiedy ocena skutków może być wymagana? | str. 116

3. Wątpliwości | str. 117

4. Wdrożenie środków mitygujących ryzyko | str. 122

5. Ocena proporcjonalności i niezbędności | str. 124

6. Konsultacje IOD | str. 128

7. Kiedy należy się konsultować z organem nadzorczym? | str. 129

8. Ustawa o ochronie danych osobowych | str. 130

9. Realizacja obowiązku i działanie w interesie publicznym | str. 131

Rozdział 6. Omówienie wpływu wystąpienia zagrożenia na prawa lub wolności osób fizycznych na przykładzie naruszenia zasad ogólnych | str. 132

1. Jak zmienia się ryzyko w przypadku braku realizacji zasad ogólnych przetwarzania danych osobowych? | str. 132

2. Które ryzyka w przypadku braku realizacji zasad przetwarzania danych osobowych z art. 5 RODO mogą wpływać bardziej na osoby fizyczne? | str. 144

Rozdział 7. Wykorzystanie norm ISO przy ocenie ryzyka i doborze środków | str. 146

1. Możliwość wykorzystania norm ISO | str. 146

2. Zarządzanie ryzykiem i wdrożenie środków mitygujących ryzyko | str. 148

3. Bezpieczeństwo i prywatność | str. 149

4. Bezpieczeństwo i prywatność ISO a NIST | str. 150

Część 2

Praktyczne przykłady

Praktyczny przykład nr 1. Świadczenie usług drogą elektroniczną, w tym zapłata danymi za usługę | str. 153

Praktyczny przykład nr 2. Chatbot | str. 180

Praktyczny przykład nr 3. System do zgłaszania wniosków | str. 196

Praktyczny przykład nr 4. Wizyty lekarskie | str. 202

Praktyczny przykład nr 5. Aplikacja mobilna | str. 208

Praktyczny przykład nr 6. Inteligentne zegarki | str. 215

Praktyczny przykład nr 7. Aplikacja do monitorowania aktywności | str. 221

Praktyczny przykład nr 8. System zarządzania wypożyczeniami samochodów | str. 231

Praktyczny przykład nr 9. Przechowywanie danych w systemach IT | str. 237

Praktyczny przykład nr 10. Dokumentacja medyczna | str. 260

Praktyczny przykład nr 11. Zarządzanie flotą | str. 280

Praktyczny przykład nr 12. Praca zdalna | str. 326

Praktyczny przykład nr 13. Rekrutacja | str. 346

Praktyczny przykład nr 14. Metoda analizy ryzyka DAPR – studium przypadku | str. 370

Bibliografia | str. 423

O autorach | str. 429