

Spis treści

Wykaz skrótów	IX
Bibliografia	XIII
Wybrane orzecznictwo	XXI

Część I. Ochrona i dostęp do informacji w cyberprzestrzeni

Rozdział I. Cyberprzestrzeń jako przestrzeń przetwarzania i wymiany informacji w systemach teleinformatycznych	3
§ 1. Pojęcie cyberprzestrzeni	3
§ 2. Obowiązki informacyjne podmiotów publicznych – przesłanki dostępu do informacji	9
§ 3. Udzielanie informacji z wykorzystaniem systemu teleinformatycznego	20
I. Strony WWW i BIP oraz centralne repozytorium danych publicznych	22
II. Informacja na wniosek – wykorzystanie poczty elektronicznej, podpisu elektronicznego, profilu zaufanego	23
1. Udostępnienie informacji publicznej na wniosek przy wykorzystaniu poczty elektronicznej	24
§ 4. Podpis elektroniczny	26
§ 5. Profil zaufany	28
§ 6. Ponowne wykorzystanie informacji sektora publicznego – <i>ratio legis</i>	31
I. Dostęp bezwarunkowy – zakres informacji przeznaczonych do ponownego wykorzystania	32
II. Informacja sektora publicznego	37
III. Ograniczenia ponownego wykorzystania	44
Rozdział II. Ograniczenia jawności informacji w cyberprzestrzeni	51
§ 1. Ochrona informacji w cyberprzestrzeni	51
§ 2. Ochrona informacji niejawnych	54
§ 3. Ochrona tajemnicy przedsiębiorstwa i prywatności	59
I. Tajemnica przedsiębiorcy	59
II. Ochrona prywatności	66
§ 4. Ochrona innych tajemnic ustawowo chronionych	69

Część II. Ochrona danych osobowych w cyberprzestrzeni

Rozdział I. Dane osobowe w cyberprzestrzeni	75
§ 1. Zasady ochrony danych w cyberprzestrzeni – źródła regulacji	75
§ 2. Zasady ochrony danych i usług w cyberprzestrzeni	77
§ 3. Ochrona danych osobowych jako zadanie z zakresu cyberbezpieczeństwa	80
§ 4. Źródło pochodzenia danych osobowych	85
§ 5. Kategorie danych osobowych	91
Rozdział II. Prawo do (ochrony) danych osobowych – charakterystyka	105
§ 1. Majątkowy i niemajątkowy charakter prawa	105
§ 2. Przenoszalność prawa do danych osobowych a przenoszalność danych	110
§ 3. Rynek danych osobowych jako nowy rynek gospodarczy – reguły obrotu	119
Rozdział III. Przetwarzanie danych osobowych – rodzaje operacji na danych osobowych	125
§ 1. Charakter i zakres czynności przetwarzania danych osobowych w cyberprzestrzeni	125
§ 2. Zautomatyzowane przetwarzanie danych osobowych	128
I. Profilowanie	132
II. Pseudonimizacja	135
Rozdział IV. Przesłanki legalizujące przetwarzanie danych w cyberprzestrzeni	137
§ 1. Przetwarzanie danych w cyberprzestrzeni	137
§ 2. Zgoda	138
§ 3. Niezbędność wykonania umowy	145
§ 4. Wypełnienie obowiązku prawnego ciążącego na administratorze jako przesłanka legalizująca	146
§ 5. Ochrona żywotnych interesów osoby, której dane dotyczą, jako przesłanka legalizująca	147
§ 6. Wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi	148
§ 7. Realizacja prawnie usprawiedliwionych interesów jako przesłanka legalizująca przetwarzanie danych osobowych	149

**Część III. Cyberbezpieczeństwo a autonomia
informacyjna i ochrona danych osobowych**

Rozdział I. Ograniczenia stosowania przepisów o ochronie danych osobowych w Krajowym Systemie Cyberbezpieczeństwa	153
§ 1. Zadania i obowiązki podmiotów wchodzących w skład systemu cyberbezpieczeństwa – zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)	153
I. Zadania CSIRT MON	156
II. Zadania CSIRT GOV	157
III. Zadania CSIRT NASK	158
§ 2. Zadania zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)	159
§ 3. Zasady udostępniania informacji i przetwarzania danych osobowych	163
Rozdział II. Dostawca usług (kluczowych i cyfrowych) jako administrator danych osobowych	167
§ 1. Realizacja celów bezpieczeństwa państwa (bezpieczeństwa narodowego) jako przesłanka modyfikująca zadania w zakresie ochrony danych osobowych	167
§ 2. Status operatora usług kluczowych i dostawcy usług cyfrowych jako administratorów danych osobowych	175
§ 3. Polityka bezpieczeństwa danych	183
§ 4. Szacowanie ryzyka naruszenia danych	188
Rozdział III. Status administratora i procesora	197
§ 1. Administrator	197
§ 2. Procesor (podmiot przetwarzający)	200
Rozdział IV. Autonomia informacyjna w cyberprzestrzeni	203
§ 1. Uwagi ogólne	203
§ 2. Prawo dostępu do danych osobowych (art. 15 RODO)	204
§ 3. Prawo do sprostowania danych osobowych (art. 16 RODO)	205
§ 4. Prawo do bycia zapomnianym i usunięcia danych (art. 17 RODO) .	207
§ 5. Prawo do ograniczenia przetwarzania (art. 18 RODO)	209
§ 6. Prawo do przenoszenia danych (art. 20 RODO)	210
§ 7. Prawo do sprzeciwu (art. 21 RODO)	211
§ 8. Prawo do ingerencji ludzkiej	212
Rozdział V. Inspektor ochrony danych osobowych	215
§ 1. Powołanie inspektora ochrony danych	215

§ 2. Status inspektora ochrony danych	217
§ 3. Zadania inspektora ochrony danych	218
Część IV. Bezpieczeństwo usług łączności elektronicznej – aspekty prawne	
Rozdział I. Bezpieczeństwo usług łączności elektronicznej	221
§ 1. Uwagi ogólne	221
§ 2. Europejska Agencja do spraw Bezpieczeństwa Sieci i Informatyki	231
§ 3. Obowiązki i odpowiedzialność przedsiębiorcy telekomunikacyjnego a bezpieczeństwo usług	234
§ 4. Tajemnica telekomunikacyjna	245
§ 5. Retencja danych w Prawie telekomunikacyjnym	255
§ 6. Charakter czynności operacyjno-rozpoznawczych a retencja danych	270
§ 7. Czynności operacyjne a ochrona praw jednostki w świetle standardów międzynarodowych	282
§ 8. Ochrona prywatności informacyjnej a przetwarzanie danych o ruchu, danych o lokalizacji i innych identyfikujących użytkownika danych	286
§ 9. Bezpieczeństwo systemów teleinformatycznych – certyfikacja i akredytacja	303
Indeks rzeczowy	315