

Spis treści

Table of Contents	XVII
Wykaz autorów	XIX
Wykaz skrótów	XXI
Wykaz literatury	XXV
Wstęp	XXXVII

Część I. Uwagi wprowadzające do roli dobrych praktyk

Rozdział I. Wprowadzenie do tematyki społecznej odpowiedzialności biznesu i kodeksów dobrych praktyk	3
§ 1. Wprowadzenie, cel opracowania	3
§ 2. Etyka w biznesie	4
§ 3. Historia społecznej odpowiedzialności biznesu	6
§ 4. Pojęcie społecznej odpowiedzialności biznesu	11
§ 5. ISO 26000	16
§ 6. Wybrane narzędzia społecznej odpowiedzialności biznesu	16
§ 7. Wdrażanie zasad społecznej odpowiedzialności biznesu	18
§ 8. Korzyści z wdrażania zasad społecznej odpowiedzialności biznesu ..	19
§ 9. Społeczna odpowiedzialność biznesu w badaniach	21
§ 10. Polskie przykłady społecznej odpowiedzialności biznesu	27
I. „L'Oréal Polska dla Kobiet i Nauki przy wsparciu Polskiego Komitetu do spraw UNESCO”	27
II. Świadoma energia RWE	28
III. Program „Tak! Pomagam”	29
IV. Fundusz Kropki Beskidu	31
§ 11. Kodeksy dobrych praktyk	32
I. Definicje	32
II. Funkcje kodeksów dobrych praktyk	34
III. Historia kodeksów dobrych praktyk	34
IV. Niektóre polskie kodeksy dobrych praktyk	35
§ 12. Wnioski	39

Rozdział II. Kodeksy dobrych praktyk w krajach o systemach <i>common law</i> – na przykładzie brytyjskich standardów w zakresie konsultacji społecznych	45
§ 1. Cel opracowania	45
§ 2. Krótkie wprowadzenie do systemu <i>common law</i>	45
§ 3. Brytyjskie kodeksy dobrych praktyk w zakresie konsultacji społecznych	49
§ 4. Rekomendacje dla Polski w zakresie konsultacji społecznych	62
Rozdział III. Mowa nienawiści w prawie polskim – postulaty <i>de lege lata</i> i <i>de lege ferenda</i>	69
§ 1. Mowa nienawiści – ujęcie ogólne	69
§ 2. Pojęcie mowy nienawiści w prawodawstwie unijnym	70
§ 3. Regulacja mowy nienawiści w prawie polskim	72
I. Regulacje karnoprawne	72
II. Regulacje cywilnoprawne	79
§ 4. Zakończenie	81
Część II. Ochrona prywatności w usługach geolokacyjnych	
Rozdział I. Unijne ramy ochrony prywatności w kontekście zagrożeń związanych z korzystaniem z usług geolokacyjnych	85
§ 1. Wprowadzenie do problematyki ochrony danych geolokacyjnych	85
1. Stopień rozwoju nowych technologii a sposoby przetwarzania danych	88
§ 2. Rodzaje infrastruktur geolokacyjnych	89
§ 3. Konieczność zapewnienia odpowiedniego stopnia ochrony prywatności	91
§ 4. Uregulowanie prawne zagadnienia ochrony prywatności w kontekście wykorzystywania danych geolokacyjnych	94
§ 5. Podsumowanie	97
Rozdział II. Geolokalizacja za pomocą urządzeń mobilnych w świetle ochrony danych osobowych	99
§ 1. Funkcjonalności urządzeń mobilnych	99
§ 2. Cele i metody ustalania lokalizacji	101
§ 3. Pozorność zgody	103
§ 4. Prawny chaos informacyjny	106
§ 5. Rola prawa bezwzględnie obowiązującego	109
§ 6. Ekwiwalentność świadczeń	110
§ 7. Nierównowaga ekonomiczna i informacyjna	112

Rozdział III. Dobre praktyki organów administracji publicznej w dostępie do geoinformacji w świetle ustawy o infrastrukturze informacji przestrzennej	115
§ 1. Wprowadzenie	115
§ 2. Dane przestrzenne jako informacja publiczna	116
§ 3. Pojęcie informacji geoprzestrzennej	118
§ 4. Obowiązki organów administracji publicznej w zakresie udostępniania danych przestrzennych	122
§ 5. Zakończenie	129
Rozdział IV. Niemiecki Kodeks ochrony danych osobowych w usługach danych przestrzennych	131
§ 1. DKGD jako Kodeks dobrych praktyk	131
§ 2. Ochrona danych osobowych w usługach danych przestrzennych	132
I. Dane i usługi danych przestrzennych	132
II. Dane osobowe	134
III. Przetwarzanie danych przestrzennych/osobowych	135
1. Autonomia informacyjna jednostki a zewnętrzny obraz nieruchomości	136
2. Autonomia informacyjna jednostki a wewnętrzny obraz nieruchomości	138
3. Powiązanie (obrazu) nieruchomości z konkretną osobą	140
§ 3. Kodeks ochrony danych osobowych w usługach danych przestrzennych	141
I. DKGD jako samoregulacja przedsiębiorstw	141
II. Cel DKGD	143
III. Zakres zastosowania DKGD	144
1. Konflikty między posiadaczami „domów”	144
2. Kontrowersje terminologiczne	147
IV. Prawa i zobowiązania sygnatariuszy DKGD	148
V. Ocena okresowa i zmiany w DKGD	149
§ 4. Projekt zmian przepisów ustawowych	151
§ 5. Podsumowanie	152
Rozdział V. Dobre praktyki w zakresie tworzenia i wykorzystania danych geodezyjnych i kartograficznych	153
§ 1. Wprowadzenie	153
§ 2. Dane geodezyjne i kartograficzne	154
§ 3. Praktyczne przykłady wykorzystania danych przestrzennych	155
§ 4. Dobre praktyki w zakresie tworzenia baz danych kartograficznych i geodezyjnych	157

§ 5. Dobre praktyki w obszarach wykorzystania danych kartograficznych i geodezyjnych	159
§ 6. Zakończenie	161

Część III. Tajemnica zawodowa

Rozdział I. Tajemnica adwokata i radcy prawnego w świetle norm etyki zawodowej	165
§ 2. Ustawowy zakres tajemnicy adwokata i radcy prawnego	167
§ 3. Tajemnica adwokata i radcy prawnego w kodeksach etyki zawodowej	170
§ 4. Odpowiedzialność dyscyplinarna za naruszenie obowiązku zachowania tajemnicy adwokata i radcy prawnego	178
§ 5. Zakończenie	179

Rozdział II. Dobre praktyki w zakresie poufności mediacji w sprawach gospodarczych	181
§ 1. Wprowadzenie do problematyki mediacji w sprawach gospodarczych	181
§ 2. Poufność jako kluczowa zasada mediacji	182
§ 3. Poufność mediacji na gruncie prawa unijnego	183
§ 4. Modele rozwiązywania konfliktów	184
§ 5. Stanowisko doktryny	185
§ 6. Poufność mediacji na gruncie prawa polskiego	187
§ 7. Konsekwencje naruszenia zasady poufności	189
§ 8. Wnioski	189

Rozdział III. Zasady etyki zawodowej w stosunkach biznesowych	191
§ 1. Wprowadzenie	191
§ 2. Zasadność tworzenia kodeksów etyk zawodowych	193
§ 3. Autonomia korporacji zawodowych	198
§ 4. Kodeksy etyczne przedsiębiorstw	200
§ 5. Etyka w biznesie	201
§ 6. Etyka w biznesie jako dział etyki stosowanej	202
I. Uzasadnienie aksjologiczne	203
II. Koncepcja utylitarna	203
III. Kodeks etyczny a koncepcja sprawiedliwości	204
§ 7. Wnioski na temat aksjologii etyki biznesowej	205

Część IV. Dostęp do informacji sądowej

Rozdział I. Kodeks dobrych praktyk dla sądownictwa w zakresie udostępniania informacji o sprawach	211
--	------------

Spis treści

§ 1. Wprowadzenie	211
I. Problemy sądownictwa	211
II. Strategia modernizacji przestrzeni sprawiedliwości w Polsce na lata 2014–2020	215
III. Kodeksy dobrych praktyk dla sądownictwa	217
IV. Cel opracowania	220
§ 2. Zarządzanie informacją sądową	221
I. Wprowadzenie systemu teleinformatycznego obsługującego biurowość elektroniczną	221
II. Wysyłanie pism sądowych bez podpisu własnoręcznego i centra druku wspólnego	225
III. Elektroniczne potwierdzenie odbioru (EPO)	230
IV. Zapis dźwięku albo obrazu i dźwięku z przebiegu posiedzenia jawnego, transkrypcja, automatyczne rozpoznawanie mowy i <i>audio word spotting</i>	240
V. Wideokonferencje	245
VI. Wyszukiwanie akt sądowych za pomocą tagów RFID	248
VII. Przeglądarka zdigitalizowanych akt sądowych	250
VIII. Elektroniczny Obieg Dokumentów, Elektroniczne Zarządzanie Dokumentacją, instrukcje kancelaryjne w sądach powszechnych	253
IX. Uprawnienia w działalności finansowej sądów i uiszczaniu opłat sądowych	257
X. Uzgadnianie między sądem a prokuraturą dni wokandowych prokuratorów	261
§ 3. Udostępnianie informacji sądowej	264
I. Portal Informacyjny Sądów Powszechnych	264
II. Portal Orzeczeń Sądów Powszechnych	268
III. Udostępnianie informacji telefonicznej, system zapowiedzi głosowej IVR	271
IV. Udzielanie informacji sądowej za pomocą poczty elektronicznej albo ePUAP-u	274
V. Zamawianie akt sądowych, samodzielne utrwalanie obrazu akt i dokumentów w nich zawartych	277
VI. Udostępnianie wokandy sądowej przez Internet (i-Wokanda); elektroniczna wokanda (e-Wokanda)	279
VII. Ujednolicenie stron internetowych sądów	281
VIII. Rzecznicy prasowi sądów i kontakty sądu z mediami	283
Rozdział II. Strategie i dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem	285

§ 1. Podstawowe zagadnienia dotyczące przetwarzania informacji w systemach teleinformatycznych	285
I. Wprowadzenie	285
II. Podstawowe definicje kluczowe dla bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych	289
§ 2. Zagrożenia dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych	292
I. Wprowadzenie	292
II. Utrata zasilania	293
III. Niewłaściwe działania pracowników	293
IV. Wady oprogramowania, sprzętu i ich niewłaściwa konfiguracja	293
V. Zagrożenia społeczno-ekonomiczne i ekologiczne	293
VI. Cyberprzestępczość	294
VII. Złośliwe oprogramowanie	297
VIII. Ataki na systemy teleinformatyczne	299
§ 3. Akty o charakterze strategicznym i akty prawne z zakresu bezpieczeństwa systemów teleinformatycznych w podmiotach publicznych	300
I. Wprowadzenie	300
II. Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń	302
1. Osiągnięcie odporności na zagrożenia cybernetyczne	303
2. Radykalne ograniczenie cyberprzestępczości	308
3. Opracowanie polityki obronnej i rozbudowa zdolności w dziedzinie bezpieczeństwa cybernetycznego w powiązaniu ze wspólną polityką bezpieczeństwa i obrony (WPBiO)	310
4. Rozbudowa zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cybernetycznego	311
5. Ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE	314
6. Rozwój zdolności w zakresie bezpieczeństwa cybernetycznego i odporności infrastruktury informatycznej w państwach trzecich	316
7. Role i obowiązki	316
8. Koordynacja między właściwymi organami ds. bezpieczeństwa sieci i informacji /CERT, organami egzekwowania prawa i organami obrony	317
9. Wnioski i dalsze działania	320

III. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej	320
1. Działania Sił Zbrojnych RP w zakresie cyberbezpieczeństwa	322
2. Działania w obszarze cywilnym w zakresie cyberbezpieczeństwa	323
IV. Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej	324
V. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej	332
VI. Krajowe Ramy Interoperacyjności	341
VII. Normy (polskie, europejskie, ISO) powołane w rozporządzeniu ws. KRI	343
VIII. Grupy robocze zajmujące się bezpieczeństwem informacji na szczeblu europejskim i międzynarodowym	345
IX. Inne działania legislacyjne związane z zapewnieniem bezpieczeństwa cyberprzestrzeni RP	346
X. Raport Najwyższej Izby Kontroli z czerwca 2015 r. o bezpieczeństwie w cyberprzestrzeni	348
XI. Ekspertyza NASK na zlecenie Ministerstwa Cyfryzacji „System bezpieczeństwa cyberprzestrzeni RP”	353
§ 4. Podsumowanie	356

Rozdział III. Dobre praktyki w zakresie udostępniania dokumentów w postaci elektronicznej w sądach powszechnych w kontekście ochrony danych osobowych

§ 1. Wprowadzenie i cel opracowania	359
§ 2. Dokument sądowy w postaci elektronicznej w postępowaniu sądowym	360
§ 3. Dobre praktyki w zakresie udostępniania dokumentów sądowych utrwalonych pierwotnie w postaci elektronicznej	361
I. Bezpieczeństwo teleinformatyczne	362
II. Zasady identyfikacji i uwierzytelnienia	363
III. Interoperacyjność	364
IV. Zasady przetwarzania danych osobowych	365
V. Kompetencje ministra sprawiedliwości w zakresie przetwarzania danych zawartych w systemach obsługujących sądy powszechne	366
§ 4. Sposoby udostępniania dokumentów sądowych w postaci elektronicznej	367
I. Portal Informacyjny	367
II. Konto w systemie teleinformatycznym (EPU)	369
III. Informatyczny nośnik danych	370
IV. Dedykowane stanowisko komputerowe w budynku sądu	371

§ 5. Wnioski końcowe i Kodeks dobrych praktyk w zakresie udostępniania dokumentów sądowych w sieci Internet	371
---	-----

Część V. Dobre praktyki w zakresie usług internetowych

Rozdział I. Dobre praktyki w zakresie dostępu do internetu i korzystania z usług internetowych	375
§ 1. Wprowadzenie, cel opracowania	375
§ 2. Czy Internet jest globalnym dobrem wspólnym?	376
I. Zarządzanie Internetem	378
§ 3. Blokowanie dostępu do Internetu	388
I. Naruszanie praw autorskich	388
II. Ochrona dzieci i młodzieży korzystających z nowoczesnych technologii	393
III. Hazard <i>on-line</i>	401
IV. Rejestr Stron i Usług Niedozwolonych	402
V. Wnioski <i>de lege ferenda</i> dotyczące blokowania dostępu do Internetu	406
VI. Samoregulacja w zakresie korzystania z Internetu	407
§ 4. Wnioski <i>de lege ferenda</i> w zakresie kodeksów etycznych dla usług internetowych	410

Część VI. Wzory dobrych praktyk

Rozdział I. Dobre praktyki w zakresie konsultacji publicznych, wpływające z wzorców brytyjskich	415
§ 1. Podstawowe zasady	415
I. Konieczność angażowania partnerów społecznych na etapie planowania legislacji	415
II. Zapewnienie pełnej przejrzystości dokumentów konsultacyjnych	416
III. Zapewnienie informacji zwrotnej	416
IV. Prowadzenie dialogu konsultacyjnego	416
V. Zapewnienie powszechnego dostępu do konsultowanych aktów	416
VI. Opracowanie przewodników i podręczników dotyczących konsultacji	417
§ 2. Dobre praktyki w zakresie planowania konsultacji społecznych	417
I. Zakres konsultacji	417
II. Podstawowe informacje	417
III. Tło	418
IV. Przedmowa	419

V. Zawartość/Spis treści	419
VI. Streszczenie i/lub wstęp	419
VII. Kluczowa część dokumentacji wraz z pytaniami	419
VIII. Podsumowanie pytań	420
IX. Dodatkowe informacje	421
X. Załączniki	421
Rozdział II. Geolokalizacja za pomocą urządzeń mobilnych w świetle ochrony danych osobowych	423
§ 1. Ocena użyteczności geolokalizacji dla użytkowników aplikacji mobilnych	423
§ 2. Dobre praktyki użytkownika urządzeń mobilnych w kontekście geolokalizacji	425
Rozdział III. Dobre praktyki w zakresie tworzenia i wykorzystania baz danych przestrzennych	427
§ 1. Tworzenie baz danych przestrzennych	427
I. Interoperacyjność danych geodezyjnych i kartograficznych	427
II. Metadane	428
III. Tworzenie systemów informacyjnych udostępniających dane przestrzenne	428
§ 2. Wykorzystanie baz danych przestrzennych	429
I. Publikacja map w Internecie	429
II. Dostęp do baz danych przestrzennych	429
III. E-usługi	429
IV. Zgłaszanie prac geodezyjnych	430
V. Polityka bezpieczeństwa	430
Rozdział IV. Zbiór dobrych praktyk w procesie udostępniania danych przestrzennych	433
§ 1. Przedmiot udostępnienia	433
§ 2. Zasadność procesu udostępnienia	433
§ 3. Sposób udostępnienia	434
§ 4. Powszechność procesu udostępniania	434
§ 5. Elektroniczny charakter procesu udostępnienia	435
§ 6. Nieodpłatność i ograniczona bezpłatność procesu udostępnienia	435
§ 7. Postulaty w zakresie bezpieczeństwa danych udostępnianych za pomocą środków komunikacji elektronicznej (zapewnienie bezpieczeństwa danych w Internecie)	436
Rozdział V. Dobre praktyki w zakresie przestrzegania tajemnicy adwokata i radcy prawnego	439

Rozdział VI. Dobre praktyki w zakresie prowadzenia mediacji w sprawach gospodarczych	441
§ 1. Dobre praktyki mediatora	441
§ 2. Dobre praktyki w postępowaniu mediacyjnym	443
§ 3. Dobre praktyki legislatora	444
Rozdział VII. Dobre praktyki w negocjacjach biznesowych oraz dobre praktyki negocjatora	445
§ 1. Dobre praktyki negocjacyjne	445
§ 2. Dobre praktyki negocjatora	446
Rozdział VIII. Dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem – dla organizacji publicznych i prywatnych	449
§ 1. Dobre praktyki z obszaru organizacyjnego	449
§ 2. Dobre praktyki z obszaru szkolenia użytkowników w organizacji	452
§ 3. Dobre praktyki z obszaru technicznego	452
I. Zróżnicowanie poziomu zabezpieczeń	452
II. Zabezpieczenie przed utratą zasilania i utratą danych	453
III. Logowanie do serwisów internetowych	453
IV. Dobre praktyki z zakresu ochrony przed atakami typu <i>phishing</i>	454
V. Dobre praktyki z zakresu ochrony przed atakami socjotechnicznymi	454
VI. Dobre praktyki z zakresu ochrony przed atakami DDoS	454
VII. Dobre praktyki z zakresu ochrony usług elektronicznych świadczonych w sieci Internet	455
VIII. Dobre praktyki z obszaru poczty elektronicznej	455
IX. Dobre praktyki dotyczące stosowania urządzeń mobilnych w organizacji	455
X. Dobre praktyki dotyczące stosowania pamięci USB w organizacji	456
XI. Dobre praktyki dotyczące tworzenia haseł	456
XII. Pozostałe dobre praktyki z obszaru technicznego	458
§ 4. Dobre praktyki z obszaru współpracy z organizacjami zewnętrznymi przy budowie systemów lub usług informatycznych .	459
Rozdział IX. Kodeks dobrych praktyk w zakresie zarządzania informacją sądową i jej udostępniania	461
§ 1. Zarządzanie informacją sądową	461
I. Oprogramowanie repertoryjno-biurowe	461

II. Centra usług wspólnych	462
III. Elektroniczne potwierdzenie odbioru (EPO) i inne doręczenia	463
IV. Zapis dźwięku albo obrazu i dźwięku z przebiegu posiedzenia jawnego, transkrypcja, automatyczne rozpoznawanie mowy i <i>audio word spotting</i>	463
V. Wideokonferencje	464
VI. Wyszukiwanie akt sądowych za pomocą tagów RFID	464
VII. Przeglądarka zdigitalizowanych akt sądowych	464
VIII. Elektroniczny obieg dokumentów, elektroniczne zarządzanie dokumentacją, instrukcje kancelaryjne	464
IX. Usprawnienia w działalności finansowej sądów i uiszczaniu opłat sądowych	465
X. Uzgadnianie między sądem a prokuraturą dni wokandowych prokuratorów	465
§ 2. Udostępnianie informacji sądowej	465
I. Portal Informacyjny Sądów Powszechnych	465
II. Portal Orzeczeń Sądów Powszechnych	466
III. Udostępnianie informacji telefonicznej, system zapowiedzi głosowej IVR	466
IV. Udzielanie informacji sądowej za pomocą poczty elektronicznej albo ePUAP-u	466
V. Zamawianie akt sądowych, samodzielne utrwalanie obrazu akt i dokumentów w nich zawartych	467
VI. Udostępnianie wokandy sądowej przez Internet (i-Wokanda); e-Wokanda	467
VII. Ujednolicenie stron internetowych sądów	468
VIII. Rzecznicy prasowi sądów i kontakty sądu z mediami	468
Rozdział X. Katalog dobrych praktyk w zakresie udostępniania dokumentów w postaci elektronicznej w sądach powszechnych w kontekście ochrony danych osobowych	469
§ 1. System teleinformatyczny obsługujący postępowania sądowe. Zasada jednego okienka	469
§ 2. Identyfikacja użytkownika i zasady przetwarzania danych	470
§ 3. Relacja na linii urząd-obywatel.	470
Rozdział XI. Kodeks dobrych praktyk w zakresie korzystania z usług internetowych	471
§ 1. „Dekalog” korzystających z usług internetowych	471
§ 2. Kultura osobista	472
§ 3. Kontrola rodzicielska wobec dzieci i młodzieży	472

Spis treści

§ 4. Poczta elektroniczna	474
§ 5. Fora internetowe	476
§ 6. Komunikatory internetowe	476
§ 7. Tworzenie bloga	477
§ 8. Czytanie bloga i jego komentowanie	478
§ 9. Tworzenie stron WWW	478
§ 10. Publikacja strony WWW	479
§ 11. Utrzymanie strony WWW	480
Indeks rzeczowy	481