

ANALIZA RYZYKA I BEZPIECZEŃSTWO DANYCH W KANCELARIACH PRAWNYCH

redakcja naukowa Dominik Lubasz

Roman Bieda, Edyta Bielak-Jomaa, Witold Chomiczewski
Włodzimierz Chróścik, Marcin Ciemiński, Agnieszka Gajewska-Zabój
Maciej Gawroński, Jarosław Greser, Damian Karwala, Damian Klimas
Maciej Kołodziej, Dominik Lubasz, Michał Magdziak, Iga Małobęcka-Szwast
Arwid Mednis, Dominika Nowak, Robert Pająk, Marcin Rojszczak
Marlena Sakowska-Baryta, Grzegorz Sibiga, Paweł Skuczyński, Monika Susańko
Katarzyna Syska, Adam Szkurłat, Kamil Szpyt, Marcin Wielisiej, Tomasz Zalewski

PRAWO W PRAKTYCE

ANALIZA RYZYKA I BEZPIECZEŃSTWO DANYCH W KANCELARIACH PRAWNYCH

redakcja naukowa Dominik Lubasz

Roman Bieda, Edyta Bielak-Jomaa, Witold Chomiczewski
Włodzimierz Chróścik, Marcin Ciemiński, Agnieszka Gajewska-Zabój
Maciej Gawroński, Jarosław Greser, Damian Karwala, Damian Klimas
Maciej Kołodziej, Dominik Lubasz, Michał Magdziak, Iga Małobęcka-Szwast
Arwid Mednis, Dominika Nowak, Robert Pająk, Marcin Rojszczak
Marlena Sakowska-Baryta, Grzegorz Sibiga, Paweł Skuczyński, Monika Susałko
Katarzyna Syska, Adam Szkurłat, Kamil Szpyt, Marcin Wielisiej, Tomasz Zalewski

PRAWO W PRAKTYCE

Zamów książkę w księgarni internetowej

profinfo.pl
księgarnia internetowa

Stan prawny na 1 października 2021 r.

Recenzent

Dr hab. Dariusz Szostek, prof. UO

Wydawca

Monika Pawłowska

Redaktor prowadzący

Kinga Zając

Opracowanie redakcyjne

Anna Kunz

Projekt okładek serii

Wojtek Kwiecień-Janikowski, Przemek Dębowski


prawolubni

Ta książka jest wspólnym dziełem twórcy i wydawcy. Prosimy, byś przestrzegając przystępujących im praw. Książkę możesz udostępnić osobom bliskim lub osobiście znanym, ale nie publikuj jej w internecie. Jeśli cytujesz fragmenty, nie zmieniaj ich treści i koniecznie zaznacz, czyje to dzieło. A jeśli musisz skopiować część, rób to jedynie na użytek osobisty.

Szanujmy prawo i własność

Więcej na www.legalnakultura.pl

Polska Izba Książki

© Copyright by Wolters Kluwer Polska Sp. z o.o., 2022

ISBN 978-83-8246-657-7

Wolters Kluwer Polska Sp. z o.o.

Dział Praw Autorskich

01-208 Warszawa, ul. Przyokopowa 33

tel. 22 535 82 19

e-mail: PL-ksiazki@wolterskluger.com

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

Wykaz najważniejszych skrótów	17
-------------------------------------	----

Słowo wstępne	19
---------------------	----

Część ogólna Analiza ryzyka i bezpieczeństwo danych w kancelariach prawnych – zagadnienia ogólne

Rozdział 1

Analiza ryzyka jako element systemu ochrony danych osobowych w kancelariach prawnych	23
1. Wprowadzenie	23
2. Założenia i cele regulacji	26
3. Podejście oparte na ryzyku	28
4. Obowiązki oparte na analizie ryzyka	34
5. Przeprowadzanie i dokumentowanie analizy ryzyka	38
6. Rola inspektora ochrony danych w procesie analizy ryzyka	49
7. Podsumowanie	57
Literatura	58

Rozdział 2

Analiza ryzyka jako element bezpieczeństwa przetwarzania danych w kancelariach prawnych	63
1. Wprowadzenie	63
2. Podejście oparte na ryzyku	64
3. Rozwinięcie zasady podejścia opartego na ryzyku i jej wpływ na bezpieczeństwo danych osobowych	64

4. Zasada ochrony danych w fazie projektowania oraz zasada domyślnej ochrony danych a bezpieczeństwo w kancelarii prawnej	65
5. Analiza ryzyka i jej wpływ na bezpieczeństwo danych na podstawie art. 32 RODO	67
6. Ocena skutków dla ochrony danych i uprzednie konsultacje (art. 35–36 RODO)	71
7. Znaczenie analizy ryzyka w przypadku wystąpienia naruszenia ochrony danych osobowych i dobór środków zaradczych (art. 33 i 34 RODO)	75
7.1. Zgłoszenie naruszenia do Prezesa UODO (art. 33 RODO)	78
7.2. Zawiadomienie osób, których dane dotyczą (art. 34 RODO)	78
7.3. Inne obowiązki administratora	79
7.4. Praktyczne przykłady naruszeń ochrony danych	79
7.4.1. Naruszenie na skutek ataku <i>ransomware</i>	80
7.4.2. Ataki polegające na wykorzystaniu danych (<i>data exfiltration attack</i>)	86
7.4.3. Naruszenie ze względu na wewnętrzne ludzkie źródło ryzyka	89
7.4.4. Naruszenie ze względu na utratę lub kradzież elektronicznych nośników informacji lub dokumentów papierowych	91
7.4.5. Naruszenie ze względu na wysłanie wiadomości do nieuprawnionych adresatów	96
7.5. Podsumowanie obowiązków związanych z zarządzaniem naruszeniami	98
8. Podsumowanie	98

Rozdział 3

Analiza ryzyka a powierzenie przetwarzania danych osobowych w kancelariach prawnych	101
1. Wprowadzenie	101
2. Kancelaria jako administrator	101
3. Cel analizy ryzyka i rola podmiotu przetwarzającego. Odpowiedzialność za analizę ryzyka	102

4. Analiza ryzyka a powierzenie przetwarzania	104
5. Postępowanie z ryzykiem w umowie powierzenia	107
6. Podsumowanie	109

Rozdział 4

Analiza ryzyka a transfery danych osobowych w kancelariach prawnych	111
1. Wprowadzenie	111
2. Reforma unijnej regulacji transferowej oraz wpływ sprawy Schrems	113
3. Zalecenia transferowe EROD 01/2020	117
4. Ocena stanu prawnego oraz praktyki w państwie trzecim	118
5. Środki uzupełniające według EROD	124
6. Transfer danych w oparciu o odpowiednie zabezpieczenia	126
7. Standardowe klauzule ochrony danych	127
8. Wiążące reguły korporacyjne	130
9. Przekazywanie danych na podstawie decyzji Komisji (art. 45 RODO)	132
10. Odstępstwa od zakazu transferu danych	136
11. Podsumowanie	139
Literatura	140

Rozdział 5

Cyberbezpieczeństwo jako element zarządzania ryzykiem kancelarii prawnych	141
1. Wprowadzenie	141
2. Kluczowe aspekty definicyjne cyberbezpieczeństwa	143
3. Źródła wymagań w zakresie cyberbezpieczeństwa	147
4. Zarządzanie cyberbezpieczeństwem według norm ISO/IEC 27000	154
5. Analiza ryzyka w cyberbezpieczeństwie	158
6. Strategie minimalizacji ryzyka	162
7. Postępowanie w przypadku wystąpienia incydentu	165
8. Podsumowanie	167
Literatura	168

Rozdział 6

Analiza ryzyka jako element zgodności ze standardami w kancelariach prawnych	169
1. Wprowadzenie	169
2. Standardy, normy i wytyczne pomocne w funkcjonowaniu kancelarii	173
3. Analiza ryzyka	183
3.1. Definicje	183
3.2. Opracowanie wewnętrznych zasad wykonywania analizy ryzyka	188
3.3. Metodyki analizy ryzyka – przykłady	192
3.3.1. Metodyka opisowa	192
3.3.2. Metodyka jakościowa	197
3.3.3. Metodyka ilościowa	200
4. Podsumowanie	203
Literatura	205

Rozdział 7

Analiza ryzyka i bezpieczeństwo danych jako element ochrony tajemnicy zawodowej	207
1. Wprowadzenie	207
2. Tajemnica zawodowa radcy prawnego i adwokata	209
2.1. Obowiązek zachowania tajemnicy zawodowej	210
2.2. Ograniczenia obowiązku zachowania tajemnicy zawodowej	212
2.3. Osoby zobowiązane do zachowania tajemnicy zawodowej	214
2.4. Tajemnica zawodowa a inne tajemnice prawnie chronione	216
3. Środki mające na celu zapewnienie bezpieczeństwa danych i ochrony tajemnicy zawodowej	217
3.1. Stosowanie podejścia opartego na ryzyku w ochronie tajemnicy zawodowej	217
3.2. Obowiązki w zakresie zapewnienia bezpieczeństwa danych objętych tajemnicą zawodową	219
3.3. Wytyczne dotyczące ochrony tajemnicy zawodowej w innych dokumentach	224
3.4. Ochrona tajemnicy zawodowej jako element zarządzania bezpieczeństwem informacji	226

4. Szacowanie ryzyka	227
4.1. Informacje objęte tajemnicą zawodową	228
4.2. Szacowanie ryzyka dla bezpieczeństwa danych objętych tajemnicą zawodową	232
4.2.1. Identyfikacja ryzyka	233
4.2.2. Określenie wielkości ryzyka	235
4.2.3. Ocena ryzyka	236
5. Podsumowanie	237
Literatura	239

Rozdział 8

Konflikt interesów w zawodach adwokata i radcy prawnego

w perspektywie opartej na ryzyku	241
1. Wprowadzenie	241
2. Ryzyko związane z działaniem w sytuacji konfliktu interesów	245
3. Ryzyko wystąpienia konfliktu interesów	247
4. Ryzyko generowane przez narzędzia zarządzania konfliktem interesów	255
5. Podsumowanie	260
Literatura	262

Rozdział 9

Analiza ryzyka jako element systemu zgodności w kancelariach

prawnych (<i>compliance</i>)	263
1. Wprowadzenie	263
2. Pojęcie <i>compliance</i>	265
2.1. Pojęcie systemu <i>compliance</i>	271
2.2. Elementy systemu <i>compliance</i>	273
2.3. <i>Compliance</i> w kancelarii prawnej	277
2.3.1. Komunikacja wewnętrzna i szkolenia personelu	278
2.3.2. Zebranie danych o funkcjonowaniu kancelarii oraz jej otoczeniu regulacyjnym	279
2.3.3. Identyfikacja i analiza ryzyka niezgodności	282
2.3.4. Dobór odpowiednich instrumentów w ramach systemu <i>compliance</i>	282
2.3.5. Idea <i>lessons learned</i>	285
3. Miejsce analizy ryzyka w systemach <i>compliance</i>	286

4. Elementy analizy ryzyka	288
4.1. Identyfikacja ryzyka	289
4.2. Szacowanie (ocena) ryzyka	290
4.3. Reakcja na ryzyko	291
4.4. Kontrola i monitorowanie ryzyka	294
5. Podstawowe rodzaje ryzyka w działalności kancelarii prawnej i sposób zarządzania nimi	295
5.1. Ryzyko naruszenia tajemnicy zawodowej	296
5.2. Ryzyko wystąpienia konfliktu interesów	300
5.3. Ryzyko naruszenia reguł zawodowej staranności	304
5.4. Ryzyko wynikające z regulacji dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu	307
6. Podsumowanie	310
Literatura	311

Część szczegółowa

Analiza ryzyka i bezpieczeństwo danych w kancelariach prawnych – wybrane zagadnienia szczegółowe

Rozdział 1

Rozwiązania chmurowe	315
1. Wprowadzenie	315
2. Pojęcie i modele chmury obliczeniowej	317
3. Wybrane zalety i wady środowisk chmurowych	320
4. Prawne i technologiczne problemy wdrożenia i korzystania z rozwiązań chmurowych	323
4.1. Umowa z dostawcą rozwiązań chmurowych	324
4.2. Ochrona danych osobowych	327
4.3. Cyberbezpieczeństwo	330
4.4. Tajemnica zawodowa	334
5. Podsumowanie	335
Literatura	336

Rozdział 2

Poczta elektroniczna	339
1. Wprowadzenie	339
2. Obowiązek zapewnienia bezpieczeństwa poczty elektronicznej	341

2.1. Obowiązek zachowania tajemnicy zawodowej	341
2.2. Obowiązki wynikające z prawa ochrony danych osobowych	344
2.2.1. Obowiązek zapewnienia poufności, integralności i dostępności danych osobowych i odpowiedniego zabezpieczenia danych	344
2.2.2. Obowiązki związane z wyborem takiego dostawcy i zawarciem z nim umowy powierzenia przetwarzania (art. 28 RODO)	346
3. Zagrożenia dla bezpieczeństwa informacji w związku z korzystaniem z poczty elektronicznej	347
3.1. Najczęstsze zagrożenia dotyczące poufności przesyłanej korespondencji	348
3.2. Najczęstsze zagrożenia dla systemu teleinformatycznego spowodowane naruszeniem poufności w związku z korzystaniem z poczty elektronicznej	348
4. Bezpieczeństwo korzystania z poczty elektronicznej w kancelariach prawnych – obszary problemowe i rekomendacje	351
4.1. Wybór dostawcy poczty elektronicznej i zawarcie umowy z nim	352
4.2. Sposoby ochrony przesyłanych informacji, w tym kryptograficzna ochrona informacji	356
4.3. Komunikacja z klientem, organami władzy publicznej lub innymi podmiotami	358
4.3.1. Komunikacja z klientem	358
4.3.2. Korespondencja z organami władzy publicznej lub innymi podmiotami	359
4.4. Ochrona systemu teleinformatycznego podczas korzystania z poczty elektronicznej	360
5. Podsumowanie	362

Rozdział 3

Narzędzia do komunikacji (wideokonferencje)	371
1. Wprowadzenie	371
2. Cele wykorzystania wideokonferencji	375
2.1. Co to jest usługa wideokonferencyjna	375

2.2. Wideokonferencja jako usługa przetwarzania w chmurze	377
2.3. Jakie pytania i odpowiedzi musi sobie zadać prawnik profesjonalny, decydując się na skorzystanie z usługi wideokonferencyjnej	378
3. Podstawy prawne	379
4. Prawne aspekty usługi wideokonferencji	380
4.1. Zakres danych osobowych	381
4.2. Role prawne dostawcy i klienta usługi wideokonferencyjnej	382
4.3. Obowiązki kancelarii jako klienta usługi wideokonferencyjnej	386
4.4. Powierzenie przetwarzania danych osobowych	388
4.5. Transfer danych poza EOG	391
4.5.1. Transfer danych do USA – RODO przed wyrokiem Schrems II	391
4.5.2. Privacy Shield/Tarcza Prywatności	392
4.5.3. Schrems II	392
4.5.4. Nieważność Tarczy Prywatności	393
4.5.5. Standardowe klauzule umowne	394
4.5.6. Względność standardowych klauzul umownych	395
4.5.7. (Niepomocne) rekomendacje EROD	397
4.5.8. Nowe SCC	398
4.5.9. Wniosek	398
4.6. Bezpieczeństwo przetwarzania danych	398
4.6.1. Wymogi prawne	398
4.6.2. Co to jest bezpieczeństwo danych i informacji	400
4.6.3. Stan wiedzy technicznej	402
4.6.4. Podstawowe środki bezpieczeństwa	404
4.6.5. Zabezpieczenie przesyłanych i przechowywanych danych	404
4.6.6. Uwierzytelnianie użytkowników	406
4.6.7. Certyfikacje bezpieczeństwa	406
4.6.8. Medialne informacje o podatnościach	407
4.7. Analiza ryzyka	407
5. Podsumowanie	411

Rozdział 4

Narzędzia do obsługi kancelarii	413
1. Wprowadzenie	413
2. Ryzyko związane ze stosowaniem narzędzi	415
3. Model oprogramowania	417
4. Projektowanie rozwiązania	419
5. Wybór dostawcy	420
6. Funkcjonalności mogące mieć istotny wpływ na ryzyko	422
7. <i>Must have</i> każdego rozwiązania	424
8. Użytkownicy	426
9. Podsumowanie	426

Rozdział 5

Obieg dokumentów	429
1. Wprowadzenie	429
2. Rola i znaczenie dokumentów w kancelarii prawnej	430
3. Obowiązki adwokata lub radcy prawnego prowadzącego kancelarię prawną w zakresie dokumentów	431
3.1. Tajemnica zawodowa	432
3.2. Ustawowe okresy retencji danych osobowych w kancelarii	438
4. Pozaprawne wymagania dotyczące obiegu dokumentów	441
5. Analiza ryzyka dotycząca obiegu dokumentów	444
6. Podsumowanie	457
Literatura	457

Rozdział 6

Podpis elektroniczny, platformy do kontraktowania	459
1. Wprowadzenie	459
2. Źródła prawa	461
2.1. Rozporządzenie eIDAS	461
2.2. Ustawa o usługach zaufania	464
2.3. Kodeks cywilny	466
3. Podpisy i pieczęcie elektroniczne	467
3.1. Podpisy elektroniczne – rodzaje	467
3.2. Pieczęcie elektroniczne	469
3.3. Podpisy elektroniczne i pieczęcie elektroniczne – skutki prawne	471

3.4. Procedura walidacyjna	472
4. Obowiązek stosowania podpisu elektronicznego w działalności adwokata i radcy prawnego	474
5. Platformy do kontraktowania	475
6. Analiza ryzyka w związku z podpisem elektronicznym	478
7. Podsumowanie	482
Literatura	482

Rozdział 7

Narzędzia automatyzujące pracę prawnika	483
1. Wprowadzenie	483
2. Podstawowe problemy we wdrażaniu automatyzacji przez prawników	485
3. Na czym polega automatyzacja?	485
4. Jakie czynności nadają się do automatyzacji?	486
5. Jak zacząć?	487
6. Wybór narzędzia do automatyzacji	490
7. Przykłady automatyzacji	492
7.1. Rejestracja nowych klientów i spraw	492
7.2. Automatyzacja dokumentów	492
7.3. Procesy zawierania umów	493
7.4. Powtarzalne doradztwo prawne	493
7.5. Komunikacja z klientem	494
7.6. Rozliczenia z klientem	494
8. Automatyzacja dla prawników oraz automatyzacja dla klientów	494
9. Podsumowanie	496
Literatura	497

Rozdział 8

Media społecznościowe	499
1. Wprowadzenie	499
2. Przedmiot analizy ryzyka i tło	500
3. Analiza ryzyka	511
3.1. Metoda proponowana przez ENISA	512
3.2. Metoda stosowana w aplikacji GDPR Risk Tracker oparta na normie ISO 29134	517

3.3. Podsumowanie dotychczasowych rozważań	525
4. Ocena skutków dla ochrony danych	525
5. Podsumowanie	527
Literatura	527

Rozdział 9

Strona internetowa kancelarii prawnej	529
1. Wprowadzenie	529
2. Regulamin a strona internetowa kancelarii prawnej	531
2.1. Regulamin świadczenia usług drogą elektroniczną i usługą świadczona drogą elektroniczną	532
2.2. Obowiązki kancelarii w przypadku świadczenia usługi drogą elektroniczną	535
3. Obowiązki kancelarii wynikające z ogólnego rozporządzenia o ochronie danych	540
3.1. Informacje, które należy przekazać użytkownikom strony www	541
3.2. Czy zgoda na przetwarzanie danych pod formularzem kontaktowym jest konieczna?	544
3.3. Hosting, czyli gdzie przechowywać dane strony internetowej?	545
4. Strona internetowa a wizerunek osób	547
5. Podsumowanie	549
Literatura	550

Rozdział 10

Organizacja pracy, w tym pracy zdalnej	551
1. Wprowadzenie	551
2. Praca zdalna	554
3. Praca zdalna – próba sprecyzowania pojęcia w kontekście organizacji kancelarii	559
4. Praca hybrydowa	562
5. Uwarunkowania organizacji pracy w kancelarii	563
6. Procedury organizacyjne – procedury pracy zdalnej	568
7. Organizacja pracy w kontekście ochrony danych osobowych	571
8. Podsumowanie	575
Literatura	576

Rozdział 11

Internet rzeczy	577
1. Wprowadzenie	577
2. Pojęcie internetu rzeczy	578
3. Główne zagrożenia bezpieczeństwa związane z korzystaniem z IoT	580
4. Wymagania prawne wdrożenia IoT w kancelarii prawnej	585
4.1. Ochrona danych osobowych	586
4.2. Cyberbezpieczeństwo	590
4.3. Prawo karne	591
4.4. Dane nieosobowe i ponowne wykorzystanie danych	592
4.5. Odpowiedzialność cywilna za szkodę wyrządzoną działaniem IoT	593
4.6. Własność intelektualna	595
5. Podsumowanie	597
Literatura	598

Rozdział 12

Narzędzia wykorzystujące sztuczną inteligencję	601
1. Wprowadzenie	601
2. Praktyczne zastosowania sztucznej inteligencji w branży prawnej	605
2.1. Zbieranie danych i komunikacja z wykorzystaniem chatbotów	607
2.2. Systemy informacji prawnej, zarządzania wiedzą oraz systemy predykcyjne	608
2.3. Analiza dokumentów i umów oraz zarządzanie umowami	610
2.4. Systemy ekspertowe	611
3. Stosowanie przepisów o ochronie danych osobowych przy wdrażaniu rozwiązań sztucznej inteligencji w kancelariach prawnych	611
4. Podejście oparte na ryzyku jako podstawa modelu wdrożeniowego	617
5. Modelowa procedura wdrożeniowa	620
6. Podsumowanie	627
Literatura	627
Autorzy	633

WYKAZ NAJWAŻNIEJSZYCH SKRÓTÓW

- ENISA** – Europejska Agencja Bezpieczeństwa Sieci i Informacji
- EROD** – Europejska Rada Ochrony Danych
- k.c.** – ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2020 r. poz. 1740 ze zm.)
- k.k.** – ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2020 r. poz. 1444 ze zm.)
- k.p.c.** – ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2021 r. poz. 1805 ze zm.)
- k.p.k.** – ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2021 r. poz. 534 ze zm.)
- KEA** – Kodeks Etyki Adwokackiej (obwieszczenie Prezydium Naczelnej Rady Adwokackiej z 27.02.2018 r. w sprawie ogłoszenia jednolitego tekstu Zbioru Zasad Etyki Adwokackiej i Godności Zawodu)
- KERP** – Kodeks Etyki Radcy Prawnego (załącznik do uchwały nr 3/2014 Nadzwyczajnego Krajowego Zjazdu Radców Prawnych z 22.11.2014 r.)
- pr. adw.** – ustawa z 26.05.1982 r. – Prawo o adwokaturze (Dz.U. z 2020 r. poz. 1651 ze zm.)
- RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Ur. UE L 119, s. 1)
- SN** – Sąd Najwyższy
- TK** – Trybunał Konstytucyjny
- TSUE** – Trybunał Sprawiedliwości Unii Europejskiej
- u.r.p.** – ustawa z 6.07.1982 r. o radcach prawnych (Dz.U. z 2020 r. poz. 75 ze zm.)
- WSA** – wojewódzki sąd administracyjny

SŁOWO WSTĘPNE

Konieczność wdrożenia systemu ochrony danych osobowych w kancelariach prawnych nie jest zagadnieniem nowym. Zobowiązania dotyczące tego obszaru wynikały pierwotnie z regulacji ustawy o ochronie danych osobowych z 1997 roku, a obecnie z obowiązującego od 25.05.2018 r. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, tzw. RODO). Realizacja tego zobowiązania napotyka jednak nadal istotne problemy, zwłaszcza w obszarze analizy ryzyka, przede wszystkim co do poprawności jej przeprowadzenia. Kancelarie prawne nie wykazują w tym zakresie znaczących odmienności niż pozostali uczestnicy obrotu należący do kategorii małych i średnich przedsiębiorców. Równocześnie istotnej modyfikacji ulega rynek usług prawnych, zarówno w obszarze organizacji procesów, jak i narzędzi, w tym wykorzystujących mechanizmy sztucznej inteligencji. Przyspieszenie transformacji cyfrowej w kancelariach prawnych, spowodowane czynnikami wywołanymi m.in. pandemią COVID-19, generuje nowe zagrożenia i zwiększa potencjalne ryzyko wymagające weryfikacji analitycznej i adekwatnego wdrożenia środków technicznych i organizacyjnych łagodzących to ryzyko.

Publikacji składa się z dwóch części. W pierwszej – przeglądowej – przedstawiono poszczególne aspekty analizy ryzyka, poczynawszy od uwag konstrukcyjnych i o charakterze ogólnym, zagadnień związanych z bezpieczeństwem, w tym w relacji z podmiotami przetwarzającymi, cyberbezpieczeństwem, zgodności ze standardami, perspektywę regulacji wewnątrz korporacyjnych oraz analizę ryzyka jako element *compliance*

w kancelariach prawnych. W drugiej, szczegółowej części w dwunastu rozdziałach omówione zostały z perspektywy analizy ryzyka i bezpieczeństwa poszczególne sposoby przetwarzania danych w kancelariach i wykorzystywane narzędzia, począwszy od rozwiązań chmurowych, poczty elektronicznej, narzędzi do komunikacji i do obsługi kancelarii, przez platformy do kontraktowania się, narzędzia automatyzujące pracę prawnika, a skończywszy na wykorzystywaniu w pracy prawnika mediów społecznościowych, stron internetowych, IoT i sztucznej inteligencji.

W publikacji uwzględniono najnowsze rozstrzygnięcia Prezesa Urzędu Ochrony Danych Osobowych, w tym w zakresie administracyjnych kar pieniężnych, a także organów nadzorczych w innych państwach członkowskich oraz orzecznictwo sądów administracyjnych i Trybunału Sprawiedliwości UE. Uwzględniono także najnowsze decyzje Komisji Europejskiej dotyczące transferów danych do państw trzecich oraz standardowych klauzul umownych w umowach powierzenia przetwarzania danych. Omówiono również wytyczne Europejskiej Rady Ochrony Danych oraz organów samorządów zawodowych radców prawnych i adwokatów.

Publikacja łączy zagadnienia teoretyczne i konstrukcyjne z kwestiami praktycznymi, które są efektem przemyśleń wielu autorów.

Wkład w opracowanie niniejszej publikacji wniosło 27 autorów o rozległych kompetencjach merytorycznych z zakresu problematyki ochrony danych osobowych, *compliance*, jak również regulacji zawodów zaufania publicznego, będących zarówno praktykami, jak i przedstawicielami nauki.

Dziękuję im za zaangażowanie i podzielenie się z czytelnikami specjalistyczną wiedzą!

Liczę, że niniejsza publikacja *Analiza ryzyka i bezpieczeństwo danych w kancelariach prawnych* będzie ciekawą propozycją wydawniczą, dostarczającą czytelnikom, zwłaszcza przedstawicielom zawodów prawniczych wykonującym zawód w kancelariach prawnych, kompleksowej wiedzy dotyczącej analizy ryzyka i bezpieczeństwa danych, oraz ułatwiającą prawidłowe stosowanie przepisów regulujących tę materię.

Dominik Lubasz

Sprawiedliwości Unii Europejskiej podkreślił jednak, że stosowanie standardowych klauzul umownych, które często są podstawą transferu danych w przypadku dostawców poczty elektronicznej z państw trzecich, może się okazać niewystarczającym mechanizmem transferowym, w szczególności gdy ustawodawstwo państwa trzeciego (np. Stanów Zjednoczonych) nie zapewnia stopnia ochrony danych osobowych merytorycznie równoważnego temu, który jest gwarantowany przez przepisy RODO. W takiej sytuacji konieczne może okazać się wdrożenie dodatkowych zabezpieczeń (środków uzupełniających). Przy implementacji postanowień wyroku TSUE w sprawie Schrems II pomocne mogą być zalecenia EROD 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych (wersja 2.0) przyjęte 18.06.2021 r. Dokument ten w założeniu ma pomóc administratorom (eksporterom danych) w ich obowiązku określenia i wdrożenia odpowiednich środków uzupełniających, jeżeli są one niezbędne do zapewnienia merytorycznie równoważnego stopnia ochrony danych przekazywanych do państw trzecich. Zalecenia zawierają plan działań (sześć kroków), jakie muszą podjąć eksporterzy danych, aby ustalić, czy muszą wdrożyć środki uzupełniające, żeby móc przesyłać dane poza EOG zgodnie z prawem UE. Zalecenia zawierają również otwarty katalog przykładowych środków uzupełniających (dodatkowych zabezpieczeń), których wdrożenie przez importera (odbiorcę) danych może zapewnić standard ochrony danych osobowych równoważny temu gwarantowanemu przez przepisy RODO.

4.2. Sposoby ochrony przesyłanych informacji, w tym kryptograficzna ochrona informacji

Adwokat i radca prawny powinni sprawdzić i być świadomi tego, w jaki sposób zabezpieczane są wiadomości e-mail, które są wysyłane z ich skrzynek poczty elektronicznej. Choć technologicznie możliwe jest wysyłanie wiadomości e-mail bez zabezpieczeń (tzw. otwartym tekstem), to z uwagi na związane z tym ryzyka dla poufności, integralności i dostępności przesyłanych informacji **nie jest rekomendowane przysyłanie wiadomości e-mail zawierających informacje poufne bez żadnych zabezpieczeń.**

Niżej przedstawione są trzy najczęściej stosowane sposoby zabezpieczenia informacji przesyłanych przy użyciu poczty elektronicznej. Zalecane jest wdrożenie co najmniej jednego z nich, w zależności od sytuacji:

- **Szyfrowanie podczas przesyłania przy użyciu protokołu TLS** (*transport-level encryption*). Zastosowanie tego zabezpieczenia oznacza, że wiadomość jest zaszyfrowana podczas jej przesyłania. Stosowanie szyfrowania podczas przesyłania zależy od ustawień serwera nadawcy oraz serwera odbiorcy – obydwie te serwery muszą mieć włączoną obsługę protokołu TLS, aby utworzone było szyfrowane połączenie na czas wysyłania wiadomości. Jeżeli serwer odbiorcy nie obsługuje protokołu TLS, to wiadomość e-mail zostanie wysłana bez zabezpieczeń. Szyfrowanie podczas przesyłania nie jest tym samym, co szyfrowanie treści wiadomości.
- **Szyfrowanie treści wiadomości *end-to-end***. W tym przypadku cała treść wiadomości jest szyfrowana przez jej nadawcę i w postaci zaszyfrowanej jest wysyłana do odbiorcy, który jako jedyny może ją odszyfrować i odczytać. Szyfrowanie całej treści wiadomości zapewnia najlepszą ochronę poufności i integralności wiadomości. Stosowanie szyfrowania *end-to-end* wymaga wdrożenia tego rozwiązania zarówno przez nadawcę, jak i odbiorcę (konieczna jest wymiana kluczy szyfrujących między nadawcą a odbiorcą).
- **Szyfrowanie załączników do wiadomości e-mail**. Jest to sposób zabezpieczenia niezależny od powyższych rozwiązań i polega na zaszyfrowaniu załącznika do wiadomości e-mail i przesłaniu go w takiej formie do odbiorcy. Hasło (klucz) do zaszyfrowanego pliku powinien być przekazany odbiorcy innym bezpiecznym kanałem (np. telefonicznie, przez SMS).

Oprócz przedstawionych wyżej sposobów zabezpieczenia informacji przesyłanych przy użyciu poczty elektronicznej należy również rekomendować **oznaczenie treści wiadomości oraz załączników jako poufnych**. Choć z pewnością nie jest to zabezpieczenie przesyłanych informacji *sensu stricto*, to stanowi uzupełnienie tych zabezpieczeń i obecnie jest standardem w zakresie przesyłania informacji objętych tajemnicą zawodową.

Ważne

Do każdej wiadomości e-mail należy załączać krótką informację lub umieścić ją w stopce, że treść wiadomości jest poufna i chroniona tajemnicą zawodową, oraz zastrzec, że jeżeli osoba nie jest właściwym adresatem wiadomości, to powinna ona poinformować o tym jej nadawcę i trwale tę wiadomość usunąć. Poszczególne pliki stanowiące załączniki do korespondencji mailowej również powinny być oznaczone jako poufne i chronione tajemnicą zawodową (np. w nazwie pliku, na pierwszej stronie dokumentu).

4.3. Komunikacja z klientem, organami władzy publicznej lub innymi podmiotami

Adwokat lub radca prawny, korzystając z poczty elektronicznej do komunikacji z klientem, organami władzy publicznej lub innymi podmiotami, musi być świadomy, że w tym obszarze może dochodzić do zagrożeń dotyczących poufności, dostępności i integralności informacji prawnie chronionych. Zmaterializowanie się takich zagrożeń może mieć szczególnie dotkliwe skutki dla kancelarii prawnych, jak też dla samego klienta. Z tego względu szczególnie istotna jest odpowiednia komunikacja z klientem na temat bezpieczeństwa poczty elektronicznej.

4.3.1. Komunikacja z klientem

Dobłą praktyką w relacjach z klientem jest poinformowanie go przy rozpoczęciu współpracy (przy przyjęciu zlecenia) o zagrożeniach związanych z korzystaniem z poczty elektronicznej i prowadzeniem korespondencji między klientem a adwokatem lub radcą prawnym za pomocą tego kanału komunikacji.

Rekomendowane jest zwrócenie klientowi uwagi na zagrożenia, które mogą dla niego wynikać z ujawnienia korespondencji objętej tajemnicą zawodową (w tym o utracie poufności lub integralności takiej korespondencji). Zalecane jest również poinformowanie klienta, z jakich

zabezpieczeń korzysta adwokat lub radca prawny (np. że jego serwer pocztowy obsługuje szyfrowanie na poziomie transmisji za pomocą protokołu TLS). W takiej informacji można też ewentualnie wskazać, jakie są konsekwencje korzystania lub niekorzystania przez klienta z pewnych zabezpieczeń (w tym np. z serwera pocztowego zapewniającego obsługę protokołu TLS, czyli szyfrowanie wiadomości podczas przesyłania).

Ponadto klienta należałoby poinformować, że na jego życzenie możliwe jest ustalenie innych sposobów zabezpieczeń korespondencji mailowej, np. zabezpieczanie załączników do wiadomości e-mail hasłem, szyfrowanie załączników, szyfrowanie całej treści wiadomości. Jednocześnie w takiej informacji dla klienta należałoby zaznaczyć, że jeżeli klient będzie korzystał z poczty elektronicznej do przekazywania adwokatowi lub radcy prawnemu informacji poufnych bez ustalania ewentualnych dodatkowych zabezpieczeń, to klient wyraża zgodę na stosowanie takiej formy komunikacji mimo potencjalnego związanego z tym ryzyka.

Informacje przekazywane klientowi na temat zagrożeń związanych z komunikowaniem się za pośrednictwem poczty elektronicznej, jak też informacje na temat stosowanych i możliwych do zastosowania zabezpieczeń powinny być regularnie uaktualniane przy uwzględnieniu ewentualnych obowiązków prawnych, wytycznych różnych organów, a także rozwoju techniki w tym zakresie.

4.3.2. Korespondencja z organami władzy publicznej lub innymi podmiotami

Odpowiednie zabezpieczenia informacji przekazywanych pocztą elektroniczną należy stosować także w przypadku przekazywania informacji prawnie chronionych do **organów władzy publicznej** (w przypadkach, w których możliwe jest wnoszenie pism za pośrednictwem poczty elektronicznej) lub innych podmiotów (np. współpracującego prawnika, innego pełnomocnika klienta).

W przypadku organów władzy publicznej, jeżeli okaże się, że organ ma własną praktykę postępowania w odniesieniu do pism składanych za

pośrednictwem poczty elektronicznej i nie da się zastosować niektórych ustalonych z klientem sposobów zabezpieczeń (lub też ich zastosowanie spowodowałoby, że pismo nie zostałoby odczytane przez organ), rekomendowane jest zastosowanie innych środków ostrożności, takich jak dokładne sprawdzenie adresu e-mail odbiorcy czy oznaczenie załączników jako poufne. Odradza się zbędne wysyłanie pocztą elektroniczną korespondencji, która została lub ma być przekazana do organu w inny sposób (np. przez ePUAP lub za pomocą innego dedykowanego systemu teleinformatycznego udostępnionego przez organ władzy publicznej).

W przypadku komunikacji z innymi podmiotami profesjonalnymi (np. współpracownikami czy innymi pełnomocnikami klienta) należałoby przedsięwziąć takie same jak w przypadku komunikacji z klientem środki ostrożności w zakresie informowania ich o zagrożeniach związanych z korzystaniem z poczty elektronicznej i prowadzeniem korespondencji za pomocą tego kanału komunikacji. W szczególności w sytuacji, gdy adwokat lub radca prawny zamierza prowadzić regularną korespondencję z daną osobą lub zamierza przesyłać tym kanałem komunikacji szczególnie wrażliwe informacje prawnie chronione, warto upewnić się, czy ów profesjonalista dysponuje odpowiednimi zabezpieczeniami poczty elektronicznej.

4.4. Ochrona systemu teleinformatycznego podczas korzystania z poczty elektronicznej

Jak zostało wskazane wyżej, korzystanie z poczty elektronicznej może prowadzić do zagrożeń dla całego systemu teleinformatycznego kancelarii prawnej.

Na podstawie wytycznych samorządów zawodowych w innych państwach¹⁴ można sformułować następujące dobre praktyki w zakresie korzystania z poczty elektronicznej, których celem jest ochrona systemu teleinformatycznego kancelarii prawnej:

¹⁴ W tym zakresie korzystano z niemieckich, angielskich i amerykańskich dokumentów wymienionych w przypisie 2.

Konieczność wdrożenia systemu ochrony danych osobowych w kancelariach prawnych nie jest zagadnieniem nowym, jednak nadal napotyka na pewne przeszkody, zwłaszcza w obszarze analizy ryzyka, w tym w poprawności jej przeprowadzenia.

W publikacji autorzy omawiają m.in.:

- zagadnienia związane z bezpieczeństwem, np. w relacjach z podmiotami przetwarzającymi,
- kwestie cyberbezpieczeństwa,
- perspektywę regulacji wewnątrz korporacyjnych,
- ryzyko jako element *compliance* w kancelariach,
- poszczególne sposoby przetwarzania danych w kancelariach,
- wykorzystywane w pracy prawnika narzędzia: rozwiązania chmurowe, pocztę elektroniczną, narzędzia do komunikacji i do obsługi kancelarii, narzędzia automatyzujące pracę prawnika,
- korzystanie z mediów społecznościowych, stron internetowych, internetu rzeczy i sztucznej inteligencji.

W opracowaniu uwzględniono najnowsze rozstrzygnięcia Prezesa Urzędu Ochrony Danych Osobowych, w tym w zakresie administracyjnych kar pieniężnych, oraz organów nadzorczych w innych państwach członkowskich, a także orzecznictwo sądów administracyjnych i Trybunału Sprawiedliwości Unii Europejskiej. Przedstawiono też najnowsze decyzje Komisji Europejskiej dotyczące transferów danych do państw trzecich oraz standardowych klauzul umownych w umowach powierzenia przetwarzania danych, jak również wytyczne Europejskiej Rady Ochrony Danych oraz organów samorządów zawodowych radców prawnych i adwokatów.

Autorami opracowania są praktycy – adwokaci i radcowie prawni oraz teoretycy z różnych ośrodków akademickich – uznani specjaliści z zakresu ochrony danych osobowych.

Dominik Lubasz – doktor nauk prawnych; radca prawny, partner zarządzający w Lubasz i Wspólnicy – Kancelaria Radców Prawnych. Kieruje specjalizacją ochrony danych osobowych. W 2021 i 2020 r. został wyróżniony w rankingu The Legal 500 jako „Leading Individual” w kategorii „Data Privacy and Data Protection” dla obszaru Europe, Middle East & Africa. W latach 2021, 2020, 2019 i 2018 otrzymał rekomendację w rankingu Chambers and Partners Europe w kategorii „TMT Data Protection”. Autor wielu publikacji z zakresu ochrony danych osobowych i prawa nowych technologii, w tym sztucznej inteligencji.



9788382466577 W01P01

ISBN 978-83-8246-657-7



9 788382 466577

ZAMÓWIENIA:

INFOLINIA: 801 04 45 45

ZAMÓWIENIA@WOLTERSKLUWER.PL

WWW.PROFINFO.PL

Kup e-book i czytaj
w aplikacji Smarteca



CENA 119 ZŁ (W TYM 5% VAT)