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-Baryła, Grzegorz Sibiga, Paweł Skuczyński, Monika Susałko
Katarzyna Syska, Adam Szkurłat, Kamil Szpyt, Marcin Wielisiej, Tomasz Zalewski

PRAWO W PRAKTYCE

Wolters Kluwer

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-Baryła, Grzegorz Sibiga, Paweł Skuczyński, Monika Susałko
Katarzyna Syska, Adam Szkurłat, Kamil Szpyt, Marcin Wielisiej, Tomasz Zalewski

PRAWO W PRAKTYCE

Wolters Kluwer

WARSZAWA 2022

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

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@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

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

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.Urz. 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, począwszy od uwag konstrukcyjnych i o charakterze ogólnym, zagadnień związanych z bezpieczeństwem, w tym w relacji z podmiotami przetwarzającymi, cyberbezpieczeństwem, zgodności ze standardami, perspektywę regulacji wewnątrzkorporacyjnych 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 przesyłanie 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 – obydwa 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

Dobrą 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 państwach[14] 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 wewnątrzkorporacyjnych,
- 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)