KSIĘGA BEZPIECZEŃSTWA KOMUNIKACJI ELEKTRONICZNEJ W PRACY RADCY PRAWNEGO

KRAJOWA IZBA
RADCÓW PRAWNYCH

Spis treści

Wstęp

Koleżanki i koledzy, członkowie samorządu radców prawnych,

Przekazuję w wasze ręce kolejne opracowania ułatwiające praktykę prawną. Stoimy twarzą w twarz zarówno ze zmianą pracy wynikającą z epidemii, ale również związaną ze zmianami technologicznymi w komunikacji, które dokonują się na naszych oczach. Rolą Krajowej Rady Radców Prawnych jest wskazywać możliwe drogi w działalności radców prawnych. Przedstawiliśmy już dwa raporty: "Strategie konkurowania indywidualnych kancelarii radców prawnych. Jak rozwijać swoje praktyki w konkurencyjnym otoczeniu?" oraz "Indywidualne kancelarie radców prawnych w czasie kryzysu. Co robić?"

Dziś przedstawiam Państwu: Księgę bezpieczeństwa" - kolejne opracowanie Krajowej Rady Radców Prawnych skierowane do radców prawnych wykorzystujących w komunikacji zawodowej pocztę elektroniczną i programy do komunikowania się na odległość. Znajdziecie państwo na kartach tego opracowania zarówno ocenę zgodności wykorzystania usług wideokonferencyjnych: Microsoft Teams będącej częścią pakietu Microsoft 365 , Zoom 5.0, Cisco Webex do komunikacji przez radców z klientami w ramach wykonywania zawodu, analizę porównawczą ogólnej zgodności oraz niektórych elementów bezpieczeństwa aplikacji do telekonferencji, rekomendacje dla radców prawnych dotyczące bezpieczeństwa poczty elektronicznej w praktyce wykonywania zawodu radcy prawnego w kontekście obowiązku zachowania tajemnicy zawodowej oraz ochrony danych osobowych czy wreszcie stanowisko Komisji Etyki i Wykonywania Zawodu Krajowej Rady Radców Prawnych dotyczące zaleceń dla radców prawnych w zakresie stosowania jako formy kontaktu z klientami wideokonferencji

Dziś zmagamy się ze skutkami COVID-19, ale też jesteśmy świadkami przyspieszenia we wdrażaniu technologii obsługi klientów i pracy samych

kancelarii prawnych. Proces elektronizacji kontaktów pomiędzy radcami prawnymi a ich klientami, który w normalnych warunkach zająłby kilka lat, musiał odbyć się w ciągu tygodni. Kontakt za pomocą środków porozumiewania się na odległość zostanie już stałym elementem naszej pracy.

Mam nadzieję, że ekspertyz w tym opracowaniu rozwieją wątpliwości i pozwolą na szersze stosowanie tych technologii w pracy radcy prawnego. Na pierwszym miejscu każdy radca prawny powinien stawiać bezpieczeństwo komunikacji i zachowanie tajemnicy zawodowej. To kolejne opracowanie KRRP pomagające radcom prawnym utrzymać wiodącą pozycję na rynku. Jak wynika z wielu krajowych i zagranicznych raportów, opanowanie nowych technologii to dziś główne wyzwanie dla kancelarii. Atutem naszego samorządu zawsze była innowacyjność i szybkie reagowanie na zmiany. Wierzę, że to opracowanie pomoże nam znaleźć się w czołówce nowoczesnych kancelarii na polskim rynku usług prawnych.

Maciej Bobrowicz
Prezes
Krajowej Rady Radców Prawnych

Warszawa, dnia 3 kwietnia 2020 r.

Stanowisko Komisji Etyki i Wykonywania Zawodu Krajowej Rady Radców Prawnych dotyczące zaleceń dla radców prawnych w zakresie stosowania jako formy kontaktu z klientami wideokonferencji

1. Przedmiot sprawy.

W dniu 24 marca 2020r. do Komisji Etyki i Wykonywania Zawodu Krajowej Rady Radców Prawnych skierowana została prośba Prezesa Krajowej Rady Radców Prawnych Macieja Bobrowicza w sprawie wyrażenia stanowiska dotyczącego zaleceń dla radców prawnych w zakresie stosowania jako formy kontaktu z klientami wideokonferencji. Związane jest to z formułowanymi w związku ze stanem epidemii na obszarze Rzeczypospolitej Polskiej oczekiwaniami co do zalecanych przez organy samorządu zawodowego form komunikowania się z klientami, w szczególności z uwagi na wprowadzoną możliwość wykonywania przez pracowników, w szczególności radców prawnych, pracy zdalnej oraz wprowadzone zalecenia dotyczącego ograniczania kontaktów osobistych.

2. Źródła prawa i materiały wykorzystane do zajęcia stanowiska.

Dla przedstawienia stanowiska w sprawie, oparto się na następujących przepisach prawa:

1) Ustawa z dnia 6 lipca 1982r. o radcach prawnych (Dz.U. z 2020r. poz. 75 z późn. zm.) – art. 3 ust. 3 i ust. 4;

2) Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. z 2020r. poz. 374 z późn. zm.);
3) Rozporządzenie Ministra Zdrowia z dnia 20 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu epidemii (Dz.U. z 2020r. poz. 491 z późn. zm.);
4) Kodeks Etyki Radcy Prawnego - Uchwała Nr 3/2014 Nadzwyczajnego Krajowego Zjazdu Radców Prawnych z dnia 22 listopada 2014r. w sprawie Kodeksu Etyki Radcy Prawnego – art. 9, art. 15, art. 23, art. 35;
5) Regulamin wykonywania zawodu radcy prawnego – Uchwała Nr 94/IX/2015 Krajowej Rady Radców Prawnych z dnia 13 czerwca 2015r. w sprawie Regulaminu wykonywania zawodu radcy prawnego – §10 ust. 1 w związku z §2 pkt 8);

oraz wykorzystano następujące materiały:

1) Włodzimierz Chróścik, Gerard Dźwigała, Leszek Korczak, Tomasz Scheffler, Jarosław Sobutka, Anita Woroniecka, Kodeks Etyki Radcy Prawnego. Komentarz, 2. Wydanie, Wydawnictwo C.H. Beck, Warszawa 2017;
2) Tomasz Jaroszyński, Anna Sękowska, Paweł Skuczyński, Kodeks Etyki Radcy Prawnego. Komentarz, Wydawnictwo Praktyka Prawnicza, Warszawa 2016.

3. Analiza zagadnienia.

3.1. Wideokonferencja jest od wielu lat powszechnie używanym narzędziem technicznym do kontaktów radców prawnych z klientami. Obowiązujący na obszarze Rzeczypospolitej Polskiej stan epidemii przyczynia się do zwiększenia częstotliwości wykorzystania tej formy kontaktu. Nie zmienia jednak jej istoty, która polega na przesyłaniu w czasie rzeczywistym dźwięku i obrazu umożliwiających kontakt audiowizualny osób korzystających z tego narzędzia.

3.2. Przepisy prawa powszechnie obowiązującego, w szczególności ustawa z dnia 6 lipca 1982r. o radcach prawnych, ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, oraz rozporządzenie Ministra Zdrowia z dnia 20 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu epidemii nie zawierają szczególnych regulacji dotyczących zasad korzystania z narzędzia technicznego w formie wideokonferencji w wykonywaniu zawodu radcy prawnego.

Z uwagi na okoliczność, że wideokonferencja jest narzędziem technicznym używanym przy wykonywaniu zawodu radcy prawnego uwzględnienia wymagają przy

korzystaniu m.in. z tego środka komunikacji przepisy ogólne ustawy z dnia 6 lipca 1982r. o radcach prawnych, tj. art. 3 ust. 3 i 4, zgodnie z którymi radca prawny jest obowiązany zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzieleniem pomocy prawnej, przy czym obowiązek ten nie może być ograniczony w czasie. Zachowanie tajemnicy zawodowej oznacza bowiem w szczególności zabezpieczenie przekazywanych w czasie wideokonferencji informacji przed ujawnieniem w szczególności osobom nieuprawionym (niepowołanym) zarówno w czasie wideokonferencji, jak i po jej zakończeniu, z zastrzeżeniem, że pod pojęciem ujawnienia rozumieć należy dostęp do wideokonferencji, jej utrwalenie lub odtworzenie w całości lub w części w celu wykorzystania przekazanych w czasie jej trwania informacji w każdej postaci, zarówno nieprzetworzonej, jak i przetworzonej.

3.3. Uwagi wymagają również przepisy prawa wewnętrznego.

A. W pierwszej kolejności zwrócić należy uwagę na zasadę ogólną wyrażoną w art. 9 Kodeksu Etyki Radcy Prawnego, zgodnie z którą dochowanie tajemnicy zawodowej jest prawem i obowiązkiem radcy prawnego, stanowi przy tym podstawę zaufania klienta i jest gwarancją praw i wolności. Zasada ta została rozwinięta w przepisach Działu III Kodeksu w Rozdziale 1. dotyczącym tajemnicy zawodowej. Wskazać tutaj należy na przepis art. 15, który w ocenie Komisji Etyki i Wykonywania Zawodu Krajowej Rady Radców Prawnych powinien znaleźć odpowiednie zastosowanie w przypadku wideokonferencji jako środka kontaktu radcy prawnego z klientem, ale przede wszystkim art. 23, który stanowi, co następuje:

Art. 23
Radca prawny obowiązany jest zabezpieczyć przed niepowołanym ujawnieniem wszelkie informacje objęte tajemnicą zawodową, niezależnie od ich formy i sposobu utrwalenia. Dokumenty i nośniki zawierające informacje poufne należy przechowywać w sposób chroniący je przed zniszczeniem, zniekształceniem lub zaginięciem. Dokumenty i nośniki przechowywane w formie elektronicznej powinny być objęte odpowiednią kontrolą dostępu oraz zabezpieczeniem systemu przed zakłóceniem działania, uzyskaniem nieuprawnionego dostępu lub utratą danych. Radca prawny powinien kontrolować dostęp osób współpracujących do takich dokumentów i nośników.

Zwrócić bowiem należy uwagę, że za jedną z form utrwalania informacji uznać należy wideokonferencję z uwagi na okoliczność, iż za jej pomocą dokonywana jest czasie rzeczywistym rejestracja dźwięku i obrazu, co pozwala na dostęp zarówno do treści samej rozmowy, jak również do prezentowanych dokumentów, które mogą być widoczne i możliwe do odczytania przez jej uczestników. W przypadku utrwalenia wideokonferencji na

nośniku informacji zastosowanie powinny także znaleźć cytowane wyżej postanowienia dotyczące nośników.

Uwagi wymaga także przepis art. 35 Kodeksu Etyki Radcy Prawnego, zamieszczony wprawdzie w rozdziale dotyczącym informowania o wykonywaniu zawodu oraz pozyskiwania klientów, ale odnoszący się wprost także do wykonywania czynności zawodowych drogą elektroniczną. Podkreślić jednak należy, że w ocenie Komisji Etyki i Wykonywania Zawodu nie znajduje on zastosowania w przypadku wideokonferencji. W literaturze przedmiotu zgodnie bowiem przyjmuje się, że Kodeks Etyki Radcy Prawnego nie definiuje pojęcia „*droga elektroniczna*" i w konsekwencji „(…) *można uznać za uzasadnione posiłkowe posługiwanie się definicją „świadczenie usługi drogą elektroniczną" z ustawy z 18.7.2002r. o świadczeniu usług drogą elektroniczną* (…)." (cyt. za: Gerard Dźwigała [w:] Włodzimierz Chróścik, Gerard Dźwigała, Leszek Korczak, Tomasz Scheffler, Jarosław Sobutka, Anita Woroniecka, Kodeks Etyki Radcy Prawnego. Komentarz, 2. Wydanie, Wydawnictwo C.H. Beck, Warszawa 2017 – komentarz do art. 35 teza 10, s. 220; zob. także: Anna Sękowska [w:] Tomasz Jaroszyński, Anna Sękowska, Paweł Skuczyński, Kodeks Etyki Radcy Prawnego. Komentarz, Wydawnictwo Praktyka Prawnicza, Warszawa 2016 – komentarz do art. 35, teza 1., s. 172). Zgodnie z art. 2 pkt 4) ustawy z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną pod pojęciem świadczenia usług drogą elektroniczną rozumieć należy wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne. Z uwagi na jednoczesną obecność stron w czasie wideokonferencji przyjąć należy, że wykonywanie czynności zawodowych z wykorzystaniem tego środka komunikacji na odległość nie jest świadczeniem usług drogą elektroniczną, a zatem nie znajduje w tym przypadku zastosowania art. 35 Kodeksu Etyki Radcy Prawnego.

B. Przechodząc z kolei do Regulaminu wykonywania zawodu radcy prawnego wskazać należy, że w przypadku utrwalenia wideokonferencji na nośniku zapewnić trzeba należyte warunki jego przechowywania, zabezpieczając przed zniszczeniem, zaginięciem i przed dostępem osób niepowołanych, a to zgodnie z postanowieniami §10 ust. 1 w związku z §2 pkt 8).

4. Podsumowanie.

Wskazując na ogólną zasadę dotyczącą obowiązku przestrzegania tajemnicy zawodowej, rozumianego w szczególności jako obowiązek zachowania, zapewnienia i zabezpieczenia tej tajemnicy, Komisja Etyki i Wykonywania Zawodu Krajowej Rady Radców Prawnych dla jego potrzeb w przypadku organizacji wideokonferencji, jako formy kontaktu z klientami podnosi, co następuje:

A. Obowiązek przestrzegania tajemnicy zawodowej oznacza konieczność zapewnienia środków technicznych mających zabezpieczyć przed jej ujawnieniem, w szczególności dostępem do wideokonferencji osób nieuprawnionych (niepowołanych).

B. W przypadku organizacji wideokonferencji przez radcę prawnego zalecić należy dołożenie przez radcę prawnego staranności wymaganej od profesjonalisty w zakresie zapewnienia narzędzia posiadającego zabezpieczenia chroniące przed dostępem osób nieuprawnionych do wideokonferencji, ujawnieniem jej przebiegu, czy możliwości odtworzenia jej przebiegu, przy czym w przypadku braku wystarczającej wiedzy w tym zakresie – skorzystanie z pomocy osoby dysponującej specjalistyczną wiedzą w tym zakresie.

C. W przypadku organizacji wideokonferencji przez klienta radca prawny powinien uprzedzić go o możliwych ryzykach związanych z używaniem tego narzędzia oraz o konieczności wyboru odpowiednich zabezpieczeń.

D. W przypadku utrwalenia wideokonferencji na nośniku informacji należy postępować z nim zgodnie z zasadami określonymi w Kodeksie Etyki Radcy Prawnego oraz Regulaminie wykonywania zawodu radcy prawnego.

E. Ponadto Komisja Etyki i Wykonywania Zawodu Krajowej Rady Radców Prawnych uznaje za zasadne systematyczne zapoznawanie się radców prawnych z zaleceniami i rekomendacjami właściwych organów i jednostek organizacyjnych administracji państwowej dotyczącymi pracy zdalnej z wykorzystaniem środków komunikacji na odległość oraz rozważenie stosowania się do nich. Tytułem przykładu wskazać można na porady Urzędu Ochrony Danych Osobowych dotyczące ochrony danych osobowych podczas pracy zdalnej z dnia 17 marca 2020r. (Ochrona danych osobowych podczas pracy zdalnej, https://uodo.gov.pl/pl/138/1459, zamieszczone także na stronie internetowej Krajowej Izby Radców Prawnych: https://kirp.pl/wp-content/uploads/2020/03/ochrona-danych-osobowych-podczas-pracy-zdalnej.pdf).

Opracowanie:
r.pr. Grzegorz Wyszogrodzki

Przewodniczący
Komisji Etyki i Wykonywania Zawodu

Krajowej Rady Radców Prawnych

r.pr. Ryszard Wilmanowicz

Ocena zgodności wykorzystania usług wideokonferencyjnych: Microsoft Teams będącej częścią pakietu Microsoft 365 , Zoom 5.0, Cisco Webex do komunikacji przez radców z klientami w ramach wykonywania zawodu oraz w działalności organów samorządu radcowskiego.

OCENA ZGODNOŚCI WYKORZYSTYWANIA USŁUG WIDEOKONFERENCYJNYCH TEAMS, ZOOM, WEBEX W DZIAŁALNOŚCI RADCÓW PRAWNYCH

MACIEJ GAWROŃSKI, MICHAŁ ĆWIAKOWSKI, PATRYCJA SZURMAK

PRZYGOTOWANA NA ZLECENIE
KRAJOWEJ RADY RADCÓW PRAWNYCH

KRAJOWA IZBA
RADCÓW PRAWNYCH

Warszawa, 31 maja 2020

Dotyczy: Wykorzystanie usług wideokonferencyjnych Microsoft Teams, Zoom, Cisco Webex w działalności radców prawnych oraz organów samorządu radcowskiego

Przedstawiamy opinię prawną dotyczącą oceny zgodności wykorzystania usług wideokonferencyjnych:

1) Microsoft Teams będącej częścią pakietu Microsoft 365
2) Zoom 5.0
3) Cisco Webex

do komunikacji przez radców z klientami w ramach wykonywania zawodu oraz w działalności organów samorządu radcowskiego.

W dalszej części opinii mówiąc „radcy" mamy na myśli także samorząd radcowski, chyba że czynimy wyraźne przeciwne zastrzeżenie.

Podsumowanie

1) W naszej ocenie radcy mogą zgodnie z prawem korzystać z Teams, Zoom i Webex:
   a) dostawcy każdej z usług oferują zgodną z wymogami RODO umowę powierzenia przetwarzania danych
   b) każdy z dostawców oferuje przechowywanie danych klienta (kontent) na terenie UE
   c) każdy z dostawców przekazuje pewne dane (telemetryczne, dane tożsamościowe użytkowników, dane rozliczeniowe) poza UE na podstawie konkretnych instrumentów prawnych (Tarcza Prywatności i standardowe klauzule umowne – SCC)
   d) każdy z dostawców oferuje odpowiednie techniczne i organizacyjne środki bezpieczeństwa danych, dające przekonanie o tym, że treść komunikacji pozostanie poufna
   e) w konsekwencji każdy z dostawców zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą, o których mowa w art. 28 ust. 1 RODO
   f) każdy z dostawców daje wystarczające gwarancje poufności komunikacji.
2) Microsoft, Zoom i Cisco zapewniają techniczne i organizacyjne środki zapewniające ochronę komunikacji przed dostępem osób trzecich. Do środków tych należy szyfrowanie, mechanizmy uwierzytelniania użytkowników, zarządzanie uprawnieniami oraz narzędzia zarządzania przebiegiem spotkań. Wykorzystanie tych funkcji wymaga jednak umiejętności korzystania z usługi oraz odpowiedniej konfiguracji. W dalszej części opinii przekazujemy praktyczne wskazówki jak bezpiecznie korzystać z usługi wideokonferencyjnej.
3) Radcy powinni informować gości swoich wirtualnych spotkań o tym, w jaki sposób przetwarzane są dane osobowe gości w związku z korzystaniem z konkretnej usługi wideokonferencyjnej (art. 13 RODO). Przykładowy obowiązek informacyjny do przekazania dla gości spotkania o sposobie przetwarzania danych zaproponowaliśmy w treści opinii.

4) Z perspektywy relacji radca – gość wirtualnego spotkania, wideokonferencja jest usługą świadczoną drogą elektroniczną w rozumieniu UŚUDE. Radcy powinni udostępniać regulamin usługi wideokonferencyjnej.

Teams

5) Microsoft ma najwyższy poziom świadomości w zakresie zasad ochrony danych osobowych. W zakresie danych przesyłanych poza EOG (zarządzanych centralnie), czyli danych telemetrycznych i podstawowych danych identyfikacyjnych o użytkownikach, Microsoft od niedawna[1] uznaje się za administratora tych danych osobowych.
6) Microsoft dysponuje też największą liczbą zewnętrznych certyfikatów swoich usług chmurowych (w tym z rodziny ISO 27xxx – bezpieczeństwo informacji).
7) W przypadku Microsoft całość usług związanych z przechowywaniem danych realizowana jest przez podmioty z grupy Microsoft, co jest pewną przewagą w zakresie formalności oraz bezpieczeństwa operacyjnego (integracja wertykalna).
8) Przewagą Teams jest też fakt, że Teams jest częścią pakietu Microsoft 365, a więc też integracja z pozostałymi usługami pakietu i wygoda.
9) Natomiast Microsoft nie oferuje na tym etapie szyfrowania end to end pomiędzy uczestnikami wirtualnego spotkania.
10) Obsługa Teams nie jest dla nas do końca intuicyjna.

Webex

11) Cisco Webex jest usługą z najdłuższym stażem i w tym kontekście jest najlepiej przetestowaną usługą z omawianych.
12) Cisco wdrożyło wiążące reguły korporacyjne, co wskazuje na duży poziom świadomości zasad ochrony danych obowiązujących w UE.
13) Duże sieciowe kancelarie często korzystają właśnie z Webex.
14) 25 września 2018 Webex został przypadkowo w całości skasowany przez pracownika Cisco i musiał być odtwarzany przez kilka dni. Zakładamy, że doprowadziło to do ulepszenia procedur aktualizacji usługi.

Zoom

15) Zoom 5.0 wymusza szyfrowanie *end-to-end* (czyli na całej linii uczestnik – reszta uczestników), co jest dużą zaletą z perspektywy poufności.
16) Zoom jest w naszej ocenie najbardziej intuicyjny, co zmniejsza ryzyko błędu.
17) Przewagą Zoom jest też, że jest firmą zajmującą się wyłącznie usługą wideokonferencyjną.
18) Zoom preferuje przeglądarkę Google Chrome.
19) Zoom jest stosunkowo najkrócej na rynku (11 lat) i były zastrzeżenia do zgodności i bezpieczeństwa Zoom przed wersją 5.0, ale obecny globalny sukces rynkowy powoduje, że Zoom błyskawicznie reaguje na te zastrzeżenia, i te, o których było wiadomo, usunął. Działa tu zapewne świadomość ryzyka reputacyjnego.

[1] Wskutek audytu holenderskiego organu ochrony danych oraz postępowania Europejskiego Rzecznika Ochrony Danych, dostęp: https://www.privacy-web.nl/cms/files/2019-08/1564735776_dpia-windows-10-version-1.5-11-june-2019.pdf .

Przepisy

Opinia została przygotowana z uwzględnieniem uwarunkowań prawnych wynikających z następujących regulacji:

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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) (**RODO**);
2) ustawa z dnia 6 lipca 1982 r. o radcach prawnych (Ustawa o radcach prawnych);
3) ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (**UŚUDE**)
4) Decyzja wykonawcza Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA
5) Decyzja Komisji z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady

Dokumentacja

Opinia została przygotowana z uwzględnieniem następującej dokumentacji:

Dla usługi Microsoft Teams

1. Oświadczenie o ochronie prywatności (**https://privacy.microsoft.com/pl-pl/privacystatement**)
2. Dodatek dotyczący ochrony danych w ramach usług online Microsoft, styczeń 2020 (https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=67)
3. Regulamin świadczenia usług online, maj 2020 (https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31)
4. Opis przeglądu zasad bezpieczeństwa i compliance Microsoft Teams (https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview?view=o365-worldwide)
5. Przewodnik bezpieczeństwa Microsoft Teams (https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide?view=o365-worldwide)
6. Modele tożsamości i uwierzytelniania w Microsoft Teams (https://docs.microsoft.com/en-us/microsoftteams/identify-models-authentication?view=o365-worldwide)
7. Lista podmiotów podprzetwarzających Microsoft 365 położenie: (https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3), link bezpośredni https://servicetrust.microsoft.com/ViewPage/TrustDocumentsV3?command=Download&downloadType=Document&downloadId=926b2cf5-6b6e-43ca-9bc3-f73e961aad5f&tab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913&docTab=7f51cb60-3d6c-11e9-b2af-7bb9f5d2d913_Subprocessor_List

8. Ocena skutków dla ochrony danych w zakresie przetwarzania danych diagnostycznych - DPIA Office 365 Online and mobile Office apps (June 2019) (https://www.privacy-web.nl/cms/files/2019-08/1564735776_dpia-windows-10-version-1.5-11-june-2019.pdf)
9. Położenie danych w Teams https://docs.microsoft.com/en-us/microsoftteams/location-of-data-in-teams

Dla usługi Zoom

1. Informacja Zoom o zgodności z RODO (https://zoom.us/gdpr)
2. Polityka prywatności Zoom (https://zoom.us/privacy?zcid=1231)
3. Często zadawane pytania – szyfrowanie spotkań (https://support.zoom.us/hc/en-us/articles/201362723-Encryption-for-Meetings)
4. Regulamin świadczenia usług online (https://zoom.us/terms)
5. Umowa powierzenia przetwarzania Zoom (https://zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf)
6. Lista podmiotów Podprzetwarzających Zoom https://zoom.us/subprocessors
7. Opis zasad bezpieczeństwa Zoom (https://zoom.us/security)
8. Zoom Security Guide (https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf)
9. Zasady rejestrowania użytkowników na spotkania (https://support.zoom.us/hc/en-us/articles/211579443-Registration-for-Meetings?zcid=1231)
10. Aktualizacje Zoom (https://zoom-video.pl/aktualizacje/)

Dla usługi Webex Cisco

1. Karta przetwarzania danych osobowych w ramach Cisco Webex Meetings (https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf)
2. Oświadczenie Cisco o ochronie danych osobowych online (https://www.cisco.com/c/pl_pl/about/legal/privacy-full.html)
3. Umowa o ochronie przetwarzania danych przez Cisco (https://trustportal.cisco.com/c/dam/r/ctp/docs/dataprotection/cisco-master-data-protection-agreement.pdf)
4. Opis środków bezpieczeństwa https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html#CiscoSecurityandTrust
5. Opis zasad administrowania usługą Webex Cisco https://help.webex.com/ld-nyw95a4-CiscoWebexMeetings/Webex-Site-Administration#Manage-Users
6. Biała księga Cloud Collaboration Security // Secure Cloud Collaboration Clients // Cisco Webex Teams Application Security (https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/Cisco-Webex-Apps-Security-White-Paper.pdf)

Pod uwagę wzięto również szereg doniesień medialnych dotyczących omawianych usług.

Opinia uwzględnia treść ww. dokumentów i deklaracji na dzień jej sporządzenia.

Cele wideokonferencjonowania

Rozważane jest wykorzystywanie usług wideokonferencyjnych przez radców w celu:

1) funkcjonowania samorządu radcowskiego: odbywania spotkań, posiedzeń, zebrań, podejmowania uchwał, także w trybie tajnym
2) kontaktowania się z klientami w sprawach objętych tajemnicą zawodową
3) przeprowadzania szkoleń.

Schemat analizy

Co to jest usługa wideokonferencyjna

Teams, Zoom i Webex Cisco to tak zwane usługi widekonferencyjne. Wideokonferencję będziemy nazywali także wirtualnym spotkaniem lub po prostu spotkaniem – w zależności od kontekstu konkretnej myśli.

Z perspektywy technicznej korzystanie z usługi wideokonferencji polega na przesyłaniu między sobą przez uczestników spotkania danych, za pomocą urządzeń tych uczestników (komputer, tablet, smartfon, telewizor), przez internet, do dostawcy usługi wideokonferencji, gdzie dane te są przetwarzane i następnie przesyłane zwrotnie do uczestników spotkania – w czasie rzeczywistym.

Użytkownicy mogą instalować na swoich urządzeniach aplikacje, które ułatwiają cały proces. Nie jest to jednak zawsze konieczne. Można się też łączyć z usługą i z niej korzystać za pomocą przeglądarek internetowych.

Usługa wideokonferencji jest więc rodzajem usługi w modelu cloud computingowym. Jest to usługa typu SaaS (software as a service), czyli udostępnianie użytkownikom konkretnej funkcjonalności użytkowej (tu różnego typu komunikacji w czasie rzeczywistym) przez internet.

W ramach wideokonferencji uczestnicy spotkania mogą przesyłać obraz ze swoich kamer, dźwięku ze swoich mikrofonów, ale także tekst (chat) jak i załączniki (pliki). Mogą być też udostępniane funkcjonalności wyższego poziomu, jak na przykład głosowanie. Usługa wideokonferencji może umożliwiać też przechowywanie przesyłanych treści. Oczywiście do tego dochodzą różnego typu funkcje zarządzania komunikacją przez organizatora spotkania.

Prawne aspekty usługi wideokonferencji

Jako usługa cloud computingowa, usługa wideokonferencji rodzi następujące typowe dla cloud computingu zagadnienia prawne dotyczące przetwarzania danych osobowych oraz przetwarzania tajemnic za pomocą podmiotów trzecich[2]:

[2] O zagadnieniach tych pisaliśmy już w 2011 roku w publikacji „Cloud Computing w sektorze finansowym. Regulacje i standardy" red. Maciej Gawroński, 2011, Forum Technologii Bankowych przy Związku Banków Polskich Dostępny na stronach Forum Technologii Bankowych przy Związku Banków

(1) rola i pozycja dostawcy usługi wideokonferencji względem usługobiorcy (radcy) i gości usługobiorcy (uczestników wirtualnych spotkań) – czy i w jakim zakresie dostawca usługi jest administratorem danych czy podmiotem przetwarzającym,

(2) zarządzanie łańcuchem podwykonawców,

(3) zobowiązanie do tajemnicy i prawo do danych,

(4) „eksport danych" poza Europejski Obszar Gospodarczy,

(5) obowiązki formalne (umowa powierzenia, obowiązek informacyjny),

(6) bezpieczeństwo danych (analiza ryzyka, ocena technicznych i organizacyjnych środków ochrony danych).

Do powyższego dochodzą (mniej ważkie ale też istotne) zagadnienia **(i)** świadczenia usług drogą elektroniczną, czyli przede wszystkim formalny obowiązek (ale i praktyczna potrzeba) sporządzenia odpowiedniego

(7) regulaminu usługi wideokonferencyjnej,

jak też interesująca kwestia **(ii)** funkcjonalnej tożsamości usługi wideokonferencji z usługą telekomunikacyjną. To jednak w Polsce na dzień dzisiejszy nie ma praktycznego znaczenia, więc nie jest poruszone dalej w opinii.

Wreszcie na końcu pojawiają się też kwestie **(iii)** licencyjne, tam gdzie użytkownicy instalują aplikacje wideokonferencyjne na własnym sprzęcie. Ten aspekt również pozostaje poza zakresem opinii.

Dane osobowe

5.3.1. Kategorie danych

Dane przetwarzane przez usługi wideokonferencyjne można skategoryzować następująco:

- **podstawowe i kontaktowe dane użytkownika**: imię, nazwisko, e-mail, telefon, login, hasło, organizacja, metoda płatności, ustawienia preferencji;
- **treści/kontent:** czyli dane przesyłane przez użytkowników – rozmowy (dźwięk, obraz), czaty, pliki. Są to tzw. dane nieustrukturyzowane. Mogą zawierać „wszystko" czyli także dane szczególnych kategorii lub dane „karne";
- **dane techniczne / telemetryczne**: IP, lokalizacja i cechy sprzętu, natężenie ruchu, requesty, anomalie, itp;
- **„inne dane"**: zależne od funkcjonalności danej platformy. Na przykład MS Teams jest zintegrowany w ramach Microsoft 365, stąd analiza prawna MS Teams musi brać pod uwagę, w pewnym zakresie, pozostałe funkcjonalności Microsoft 365 (np. integrację MS Teams z kalendarzem). Co ciekawe, Microsoft 365 może być w pewnym zakresie zintegrowany z Zoom.

5.3.2. Role prawne dostawcy i klienta usługi wideokonferencyjnej

Klient administrator, dostawca przetwarzający. Dostawca usługi wideokonferencyjnej jest podmiotem przetwarzającym dane osobowe (art. 4 pkt 8 RODO, art. 28 RODO), powierzane mu przez biznesowego klienta tej usługi, który działa jako administrator danych osobowych (art. 4 pkt 7 RODO).

Polskich https://zbp.pl/dla-bankow/bankowosc-elektroniczna/forum-technologii-bankowych, link bezpośredni https://www.zbp.pl/getmedia/030dda41-69d6-4c21-9895-573edc218875/Cloud_Computing

Dostawca jako administrator. W praktyce, w pewnym zakresie dostawca usługi działa też jako administrator niektórych danych osobowych pozyskanych w związku z korzystaniem z usługi przez jej użytkowników[3]. Chodzi tu przede wszystkim o dane techniczne/telemetryczne i podstawowe dane użytkownika, dla celów zarządzania użytkownikami, raportowania finansowego oraz cyberbezpieczeństwa.

Microsoft „rozpoznał" tę swoją rolę administratora danych osobowych w nowych dokumentach usługi Microsoft 365[4] ze stycznia 2020. Było to efektem „ostrzału regulacyjnego" ze strony holenderskiego Ministerstwa Sprawiedliwości, Europejskiego Rzecznika Ochrony Danych Osobowych i niemieckich organów ochrony danych osobowych.

Cisco w oświadczeniu o ochronie danych na swoje stronie również wskazuje, że Cisco może działać jako administrator danych. Jednak zapisy podane w oświadczeniu są zbyt generyczne i nie dają odpowiedzi na jakiej podstawie prawnej i w jakim celu Cisco działa jako administrator danych.

Zoom na razie plasuje się wyłącznie w roli podmiotu przetwarzającego.

W praktyce każdy dostawca usługi chmurowej (a więc i Zoom i Cisco etc) będzie w tej samej sytuacji. Spodziewamy się więc z czasem aktualizacji także dokumentacji prawnej pozostałych (innych niż Microsoft) dostawców usług chmurowych. Z perspektywy klientów usług chmurowych ten niższy poziom świadomości regulacyjnej w obszarze europejskiej ochrony danych osobowych dostawców innych niż Microsoft nie blokuje możliwości korzystania z tych usług. Klienci usług chmurowych (radcy) powinni jedynie zadbać o przekazanie stosownych informacji gościom swoich wirtualnych spotkań.

Brak współadministrowania. W naszej ocenie w żadnym zakresie nie powstaje pomiędzy klientem a dostawcą usługi wideokonferencyjnej stosunek współadministrowania danymi osobowymi. To stwierdzenie jest istotne ze względu na kontrowersyjny wyrok Trybunału Sprawiedliwości UE z dnia 29 lipca 2019[5] wydany w sprawie C-40/17 tzw. „wyrok Fashion ID". W wyroku Fashion ID Trybunał dopatrzył się współadministrowania pomiędzy Facebookiem a operatorem strony internetowej, na której umieszczono znacznik śledzący Facebook Pixel. Wyrok krytykowaliśmy wielokrotnie. W tym miejscu nie będziemy rozwijać bezpośredniej argumentacji prawnej. Dość powiedzieć, że organy ochrony danych, które niejako „wymusiły" na Microsoft aktualizację dokumentacji zgodności na początku 2020, nie uznały Microsoft i klientów usług Microsoft 365 za współadministratorów.

5.3.3. Obowiązki klienta usługi wideokonferencyjnej

Obowiązki. Klient usługi wideokonferencyjnej (radca, organ samorządu) zawierając umowę o korzystanie z usługi wideokonferencyjnej z dostawcą tej usługi ma następujące obowiązki z obszaru ochrony danych:

1) **[wiarygodność]** sprawdzić, czy dostawca usługi „zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych" aby usługa „spełniała wymogi RODO i chroniła prawa osób, których dane dotyczą" (zgodnie z art. 28 ust. 1 RODO). Chodzi tu o weryfikację:

   a) zgodności działania usługi z prawem ochrony danych osobowych

   b) bezpieczeństwa usługi

   Sprawdzenia tego w odniesieniu do usług chmurowych klasy globalnej dokonuje się zwykle przez weryfikację dokumentów formalnych – umowy powierzenia przetwarzania danych i innych informacji podawanych przez samych dostawców, certyfikatów

[3] Dostawca usługi wideokonferencyjnej jest też administratorem danych osobowych pozyskiwanych od swoich klientów konsumenckich, co jednak pozostaje poza zakresem zainteresowania naszej opinii.
[4] Microsoft ostatnio zmienił nazwę swojego pakietu usług z Office 365 na Microsoft 365
[5] http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=1278754

niezależnych firm, jak i doniesień rynkowych na temat praktyki działania danej usługi, w tym informacji o wyciekach danych, podatnościach, awariach oraz praktykach handlu danymi.

Wykonaliśmy takie analizy i są one zamieszczone dalej w opinii.

2) **[umowa powierzenia]** sprawdzić, czy dostawca usługi oferuje umowę powierzenia przetwarzania danych, spełniającą wymogi art. 28 RODO.

   Art. 28 RODO zawiera długą listę wymogów, która jest także listą kontrolną do weryfikacji umowy powierzenia z dostawcą usługi.

3) **[eksport danych]** jeżeli dostawca usługi wideokonferencyjnej przetwarza dane poza terytorium EOG, ustalić, jakie dane są przetwarzane poza EOG i na jakich zasadach zapewniona jest zgodność tego przetwarzania z RODO (art. 44-46 RODO).

   W praktyce stosuje się dwie metody zapewnienia zgodności: (1) dostawca z USA może zgłosić się do objęcia programem US-UE Tarcza Prywatności; (2) dostawca w uzupełnieniu umowy przetwarzania danych zawiera z klientem także tak zwane Standardowe Klauzule Umowne (SCC)[6], czyli wzorzec umowny zaaprobowany przez Komisję Europejską.

   W praktyce każdy liczący się dostawca usługi wideokonferencyjnej pochodzi z USA i jakieś dane do USA transferuje. Stąd klient usługi będzie miał obowiązek informowania swoich gości o tym transferze i pewnych jego szczegółach.

4) **[obowiązek informacyjny]** należy informować gości swoich wirtualnych spotkań o tym, w jaki sposób przetwarzane są ich dane osobowe w związku ze spotkaniem (art. 13 RODO).

5) **[rozliczalność]** należy udokumentować swoją analizę, aby móc rozliczyć się ze zgodności z RODO (art. 5 ust. 2 RODO)

   Niniejsza opinia jest narzędziem do takiego „rozliczenia się" z RODO i obowiązkiem zachowania tajemnicy zawodowej.

UŚUDE

Z art. 8 UŚUDE wynika obowiązek posiadania regulaminu usługi świadczonej drogą elektroniczną.

Wideokonferencja jest w naszej ocenie usługą świadczoną drogą elektroniczną uczestnikom spotkania przez jego organizatora.

Art. 3 pkt. 6) UŚUDE wprowadza wyjątek od zastosowania reżimu UŚUDE w ramach struktury organizacyjnej usługodawcy, kiedy usługa służy wyłącznie do kierowania pracą lub procesami gospodarczymi. Stąd formalnie wirtualne posiedzenie organu samorządu radcowskiego czy też wewnętrzne spotkanie kancelarii mogłoby obejść się bez regulaminu.

Jednak regulamin jest nie tylko wymogiem formalnym, ale i potrzebnym narzędziem prawnym dla uregulowania relacji klienta usługi wideokonferencyjnej z jego wirtualnymi gośćmi. Można sobie wyobrazić sytuację, gdy uczestnicy wirtualnego spotkania, którzy mają sprzeczne interesy (np. negocjacje ugodowe) lub animozje osobiste (czysto teoretyczny przykład: dziekani różnych izb) zaczynają obrzucać się złośliwymi uwagami lub wręcz wyzwiskami. Można sobie wyobrazić również, że pracownicy kancelarii w źle pojętym celu wzmocnienia

[6] Na 16 lipca 2020 planowane jest orzeczenie Trybunału Sprawiedliwości UE co do zgodności SCC z Traktatami

komitywy z klientem wymieniają się z nim niestosownymi materiałami podczas wirtualnego spotkania.

Sporządzenie regulaminu usługi wideokonferencyjnej leży w zasadzie w całości po stronie klienta usług (radców), stąd nie stanowi ograniczenia prawnego w korzystaniu z którejkolwiek z usług wideokonferencyjnych.

Analiza poszczególnych usług

Umowa powierzenia

Teams, Zoom i Webex oferują umowę powierzenia przetwarzania danych. Umowy formalnie odpowiadają wymogom art. 28 RODO. W niżej umieszczonej tabelce przedstawiamy szczegółowe rozliczenie.

Dostawcy usług wideokonferencyjnych zgodnie (i trafnie) stawiają się w roli podmiotu przetwarzającego w odniesieniu do treści komunikowanych sobie przez uczestników spotkań za pomocą tych usług (*user generated content*).

Jak już wspomnieliśmy, Microsoft, wskutek oceny skutków dla ochrony danych zleconej w zeszłym roku przez holenderskie/niderlandzkie[7] Ministerstwo Sprawiedliwości i opracowanej 22 lipca 2019, rozpoznał swoją rolę jako administratora danych o użytkownikach i danych technicznych/telemetrycznych[8]. Dane techniczne Microsoft przetwarza w celu bezpieczeństwa i optymalizacji. Dane o użytkownikach przetwarza w celu zarządzania tożsamością użytkowników i rozliczeń. Te dane, administrowane przez Microsoft, Microsoft przetwarza centralnie, a więc eksportuje je poza EOG. Kontent (czyli dane zawierające treść komunikatów użytkowników) Microsoft przetwarza na terenie UE.

Cisco deklaruje, że może działać jako administrator „niektórych" danych, co wskazuje, że zdiagnozował problem, o którym mowa wyżej. Nie znaleźliśmy jednak szczegółowych wyjaśnień, jak Cisco to zagadnienie adresuje.

Zoom na razie nie rozpoznają swojej roli jako administratora danych, o których mowa wyżej, mimo że sytuacja prawna i faktyczna Zoom też nie różni się od sytuacji Microsoft.

Okoliczność, że Zoom „nie widzi się" w roli administratora danych, a co do Cisco nie jest to do końca jasne, nie ma w naszej ocenie wpływu na legalność korzystania z Zoom czy Webex przez radców. Umowa powierzenia zapewnia klientowi obu usług (radcy) narzędzia żądania zgodności z RODO, w tym bezpieczeństwa komunikacji.

W odniesieniu do każdej z usług radca powinien poinformować swoich wirtualnych gości o tym, w jaki sposób przetwarza ich dane osobowe w ramach usługi wideokonferencyjnej (art. 13 RODO). Nadto nawet w odniesieniu do Microsoft Teams radca powinien przekazać gościom informację o tym, że ich niektóre dane są przesyłane poza UE. Wymagają tego zasady przejrzystości i rzetelności przetwarzania danych (art. 5 ust. 1 lit. a RODO).

Analiza umów powierzenia przetwarzania MS Teams, Zoom, Webex

Lokalizacja umów powierzenia przetwarzania:

[7] Holandia ostatnio zmieniła nazwę swojego kraju. Nie do końca wiadomo, jak my ich mamy teraz po polsku nazywać.

[8] https://www.zdnet.com/article/microsofts-new-office-365-terms-we-wont-use-your-data-for-advertising-or-profiling/

1) **MS Teams.** Dodatek dotyczący ochrony danych w ramach usług online Microsoft Styczeń 2020 (dalej: **Dodatek MS**) w załączniku nr 3 zawiera uzupełnienie postanowień umowy powierzenia przetwarzania: https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=67
2) **Zoom.** Global Data Processing Addendum stanowi umowę powierzenia przetwarzania https://zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf (dalej: **DPA Zoom**)
3) **WebEx.** Master Data Protection Agreement https://trustportal.cisco.com/c/dam/r/ctp/docs/dataprotection/cisco-master-data-protection-agreement.pdf (dalej: **MDPA Webex**),
Informacje uzupełaniające w Privacy Data Sheet *(https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf)* (dalej: (**PDS**)

Lp	Wymóg RODO	MS Teams	Zoom	Webex
1.	Umowa [RODO 28.3]	Dodatek MS (uzupełniająco załącznik nr 3 do Dodatku MS)	Global Data Processing Addendum	Master Data Protection Agreement
2.	Dalsze powierzenie [RODO 28.2].	str. 10 Powiadomienie i kontrole dotyczące korzystania z usług Podmiotów Podprzetwarzających, Dodatek MS Lista dalszych przetwarzających: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2JOJ1	pk. 5.1 DPA Lista dalszych przetwarzających: https://zoom.us/subprocessors	pkt 6 Attachment B, MDPA Webex Lista dalszych przetwarzających na wniosek administratora Uzupełniająco: Informacje o dalszych przetwarzających PDS pkt. 8
3.	Zgoda na dalsze powierzenie [RODO 28.2 zd. 2].	str. 10 Powiadomienie i kontrole dotyczące korzystania z usług Podmiotów Podprzetwarzających, Dodatek MS	pkt 5.1-5.2. DPA	pkt 6.e Attachment B, MDPA Webex
4.	Sprzeciw względem dalszego powierzenia [RODO 28.2 zd. 2].	str. 10 Powiadomienie i kontrole dotyczące korzystania z usług Podmiotów Podprzetwarzających, Dodatek MS	pkt 5.1 DPA	pkt 6.b Attachment B, MDPA Webex
5.	Transfer obowiązków [RODO 28.4].	str. 10, Powiadomienie i kontrole dotyczące korzystania z usług Podmiotów Podprzetwarzających, Dodatek MS	pkt 5.4 DPA	pkt 6.d Attachment B, MDPA Webex
6.	Przedmiot [RODO 28.3]	str. 7, Szczegóły dotyczące przetwarzania, Dodatek MS	Exhibit A – Details of Processing, DPA	Scope Attachment B, MDPA Webex
7.	Czas. [RODO 28.3]	str. 7, Szczegóły dotyczące przetwarzania, Dodatek MS	Exhibit A – Details of Processing, DPA	Scope Attachment B, MDPA Webex
8.	Charakter i cel. [RODO 28.3]	str. 7 Szczegóły dotyczące przetwarzania, Dodatek MS	Exhibit A – Details of Processing, DPA	Appendix 1 to Attachment D, MDPA Webex
9.	Rodzaj danych osobowych. [RODO 28.3]	str. 7, Szczegóły dotyczące przetwarzania, Dodatek MS	Exhibit A – Details of Processing, DPA	Appendix 1 to Attachment D, MDPA Webex
10.	Kategorie osób. [RODO 28.3]	str. 7, Szczegóły dotyczące przetwarzania, Dodatek MS	Exhibit A – Details of Processing, DPA	Appendix 1 to Attachment D, MDPA Webex,
11.	Udokumentowane polecenia [RODO.28.3.a]	str. 16, Role i obowiązki podmiotu przetwarzającego i	pkt 3.1 DPA	pkt 4.d.i Attachment B, MDPA Webex

		administratora, Dodatek MS		
12.	Tajemnica. [RODO.28.3.b]	str. 10, Zobowiązanie Podmiotu Przetwarzającego do Zachowania Poufności, Dodatek MS	pkt 4.2 DPA	pkt 4.c.ii Attachment B, MDPA Webex,
13.	Przetwarzanie poza EOG [RODO.28.3.a]	str. 9, Lokalizacja i przechowywanie danych, Dodatek MS Kontent w EU, pozostałe Privacy Shield	pkt 7 DPA EXHIBIT C – Standard Contractual Clauses	pkt 5 Attachment B, Attachment D, MDPA WebEx, Kontent można umieścić w EU
14.	Bezpieczeństwo. [RODO.28.3.c]	Aneks A — Środki bezpieczeństwa, Dodatek MS	pkt 6 DPA, EXHIBIT B – Zoom minimum security control requirements	Attachment A, MDPA Webex,
15.	Współpraca przy realizacji praw jednostki. [RODO.28.3.e]	str.16, Prawa osób, których dane dotyczą; pomoc przy wnioskach, Dodatek MS	pkt 8.1-8.2 DPA	pkt 7.a Attachment B, MDPA Webex,
16.	Wsparcie przy obowiązkach bezpieczeństwa. [RODO.28.3.f].	str. 26, Stosowne obowiązki wynikające z RODO: art. 28, 32 i 33, Dodatek MS	pkt 9.1.-9.3. DPA	pkt 4.d.xi Attachment B, MDPA Webex,
17.	Analiza ryzyka przetwarzania danych osobowych. [RODO 32 RODO]	str. 16, Zasady i procedury bezpieczeństwa, Dodatek MS	pkt 6.1 DPA	pkt 4.c.i Attachment B, MDPA Webex
18.	Powiadomienie o naruszeniu [RODO 33.2]	str. 9, Powiadomienie o Naruszeniu Zabezpieczeń, Dodatek MS	pkt 9.5 DPA	pkt 4. Attachment A, MDPA Webex [powinno mieć nr 5]
19.	Audyty. [RODO 28.3.h]	str. 8, Kontrola przestrzegania postanowień, Dodatek MS	pkt 3.4 20, EXHIBIT B-Zoom minimum security control requirements	pkt 4.l.ii Attachment A, MDPA Webex
20.	Współpraca przy audytach [RODO 28.3.h]	str. 8, Kontrola przestrzegania postanowień, Dodatek MS	Customer shall rely on the third-party audit SOC 2 Type II report for validation of proper information security practices and shall not have the right to audit, except in the case of a Security Breach resulting in a material business impact to Customer. pkt 20.1, EXHIBIT B-Zoom minimum security control requirements	pkt 4.l.ii Attachment A, MDPA Webex
21.	Odpowiedzialność za Dalszego Przetwarzając	str. 10, Powiadomienie i kontrole dotyczące korzystania z usług, Podmiotów	pkt 5.5 DPA	pkt 6.d Attachment B, MDPA Webex

	ego. [RODO 28.4]	Podprzetwarzających, Dodatek MS		
22.	Usunięcie danych osobowych [RODO 28.3.g]	str. 9 i 10, Zatrzymywanie i usuwanie danych, Dodatek MS	pkt 3.4 DPA	Postanowienie 4.d.xii Attachment B, MDPA Webex – Uzupełniająco: Informacje o retencji PDS pkt. 6
23.	Obowiązek pozostawienia danych osobowych [RODO 28.3.g]	str. 9 i 10 Zatrzymywanie i usuwanie danych, Dodatek MS	pkt 3.4 3.4 DPA	Postanowienie 4.d.xii Attachment B, MDPA Webex

Transfer danych poza eog

Wszyscy dostawcy informują, że w ramach korzystania z usługi może dochodzić do przetwarzania danych poza EOG.

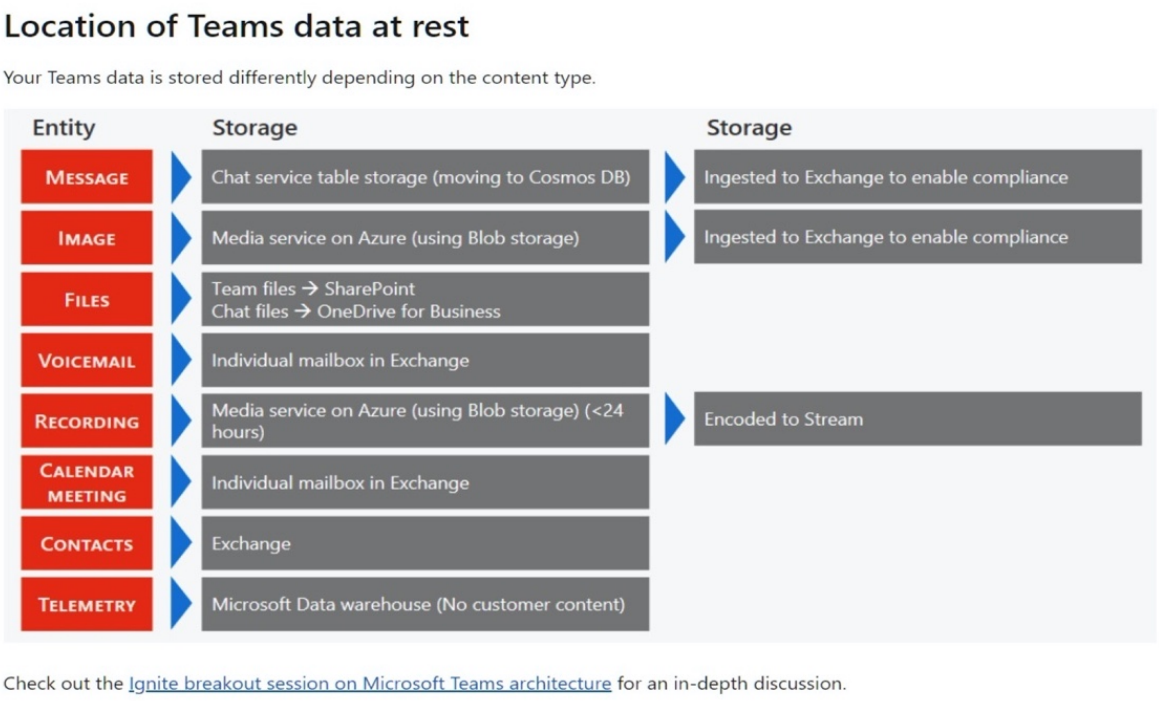
Dostawcy w swojej dokumentacji oświadczają, że użytkownicy mają możliwość wyboru lokalizacji, gdzie dane będą przechowywane.

Teams. Treści europejskich użytkowników Microsoft 365 domyślnie przechowywane są w europejskich centrach danych Microsoft (Dublin i Amsterdam). https://docs.microsoft.com/en-us/microsoftteams/location-of-data-in-teams). Zgodnie z warunkami świadczenia usług (str. 28 OST Microsoft maj 2020[9]) dane dla: Exchange, Sharepoint i Onedrive domyślnie przetwarzane są w rejonie (*Geo*) lokalizacji klienta Microsoft. Natomiast z informacji podanych na stronie Microsoft[10] oraz mapy wskazującej miejsce przetwarzania danych dla usługi Teams wynika, że właśnie w powyżej wskazanych usługach są przechowywane dane z usługi Teams. W ten nieco zawiły sposób[11] Microsoft deklaruje, że dane przetwarzane za pomocą usługi Teams są przechowywane tam, gdzie podstawowe usługi oferowane przez Microsoft. Metadane (dane techniczne) jak i dane samych użytkowników (jednolita książka adresowa) przesyłane są do USA.

[9] **Location of Customer Data at Rest for Core Online Services**
For the Core Online Services, Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as follows: Office 365 Services. If Customer provisions its tenant in Australia, Canada, the European Union, France, Germany, India, Japan, South Africa, South Korea, Switzerland, the United Kingdom, the United Arab Emirates, or the United States, Microsoft will store the following Customer Data at rest only within that Geo: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint Online site content and the files stored within that site, and (3) files uploaded to OneDrive for Business.

[10] https://docs.microsoft.com/en-us/microsoftteams/location-of-data-in-teams

[11] Jednak o niebo bardziej przejrzysty niż przed karą 57 milionów euro za brak przejrzystości nałożoną na Google 21 stycznia 2019 przez francuski organ ochrony danych CNIL.



Dla przykładu nasza Kancelaria GP przetwarza dane w Unii Europejskiej. Każdy klient Microsoft może sprawdzić w ustawieniach swojego konta, gdzie jego dane są przechowywane[12].

Zoom i Cisco Webex użytkownikom biznesowym oferują możliwość ograniczenia przetwarzania treści do centrów danych w UE. (https://support.zoom.us/hc/en-us/articles/360042411451-Selecting-data-center-regions-for-hosted-meetings-and-webinars).

[12] https://docs.microsoft.com/en-us/microsoftteams/location-of-data-in-teams

Darmowe wersje. Teams domyślnie przechowuje dane w tzw. Geo klienta usługi także w wersji darmowej (czyli w EU dla użytkowników z EU).

Korzystając z darmowej wersji Zoom jesteśmy „z automatu" przypisani do lokalizacji rejestracji naszego konta (co wskazywałoby również na UE w naszym przypadku).

W przypadku Webex, Cisco podaje informacje, że korzystając z usługi w wersji darmowej dane mogą być przetwarzane poza regionem rejestracji konta.

W odniesieniu do wszystkich dostawców usług, dane techniczne i dane o użytkownikach i tak trafiają do USA bez względu na odpłatność czy nie usługi.

Podstawy transferu danych poza EOG

Podstawy prawne transferu danych poza EOG. Przekazywanie danych osobowych poza terytorium Europejskiego Obszaru Gospodarczego zostało uregulowane w rozdziale V RODO. Taki „eksport danych" wymaga odrębnej podstawy prawnej. Zwykle stosowane są dwie podstawy prawne (często wspólnie):

(1) tak zwana Tarcza Prywatności (*Privacy Shield*) czyli zestaw narzędzi prawnych opartych o umowę międzynarodową UE – USA legalizujący transfer danych do USA lub

(2) standardowe klauzule umowne (tzw. SCC = *standard contractual clauses*, zwane również *EU model clauses*), o których mowa w art. 46 ust. 2 lit. c RODO.

Oba instrumenty mogą się na siebie nakładać.

7.1.1. Privacy Shield / Tarcza Prywatności

Art. 45 ust. 1 RODO

*Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, **gdy Komisja stwierdzi, że to państwo trzecie,** terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa **zapewniają odpowiedni stopień ochrony**. Takie przekazanie nie wymaga specjalnego zezwolenia.*

Komisja w dniu 12 lipca 2016 r przyjęła decyzję w sprawie odpowiedniej ochrony danych osobowych dla programu Tarcza Prywatności UE-USA („**Privacy Shield**").

Umowa UE-USA wprowadza możliwość tak zwanej samocertyfikacji na zgodność z prawem ochrony danych EU przez podmioty amerykańskie. Polega to na złożeniu stosownej deklaracji przez podmiot amerykański do Federalnej Komisji Handlu (Federal Trade Commission) o tym, że będzie on stosować prawo europejskie do danych europejskich. Lista podmiotów objętych Tarczą Prywatności jest publikowana w Internecie (np. tu https://www.privacyshield.gov/list).

Microsoft 365, Zoom i Cisco Webex zostały zgłoszone jako objęte przez Tarczę Prywatności i widnieją na liście podmiotów objętych Tarczą Prywatności.

7.1.2. SCC – Standardowe klauzule umowne

Art. 46 RODO

> *1. W razie braku decyzji na mocy art. 45 ust. 3 administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej.*

2. Odpowiednie zabezpieczenia, o których mowa w ust. 1, można zapewnić – bez konieczności uzyskania specjalnego zezwolenia ze strony organu nadzorczego – za pomocą:

(…)
*c) **standardowych klauzul ochrony danych przyjętych przez Komisję** zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2;*

Kolejną podstawą transferu danych poza EOG może być stosowanie przez administratora czy podmiot przetwarzający tzw. standardowych klauzul umownych (SCC, *standard contractual clauses*).

Aby skorzystać z takiego "zalegalizowania" transferu, w przypadku podmiotów mających siedzibę w kraju trzecim (czyli poza Europejskim Obszarem Gospodarczym), podmiot musi zawrzeć odpowiednią umowę zawierającą konkretne wzorce postanowień umownych (stąd nazwa „standardowe klauzule umowne") z administratorem danych osobowych z UE.

Microsoft, Zoom i Cisco stosują, równolegle do partycypacji w Tarczy Prywatności, standardowe klauzule umowne w swoich umowach z klientami z UE.

UWAGA: Na 16 lipca 2020 planowany jest wyrok Trybunału Sprawiedliwości UE w sprawie zgodności SCC z Traktatami.

7.1.3. Cisco BCR – wiążące reguły korporacyjne

Cisco deklaruje również zgodność przetwarzania danych na podstawie tzw. wiążących reguł korporacyjnych (BCR = *binding corporate rules*), zgodnie z art. 47 RODO[13].

Wiążące reguły korporacyjne (BCC) to rodzaj regulaminu przetwarzania danych zgodnie z prawem UE, przyjmowanego przez grupę przedsiębiorstw (grupę kapitałową) dla swoich firm spoza Europejskiego Obszaru Gospodarczego, tworzący jakby prywatny obszar zgodności z europejską ochroną danych. Jest to instrument prawny o ciekawej naturze. BCC na przykład nie wymagają umów pomiędzy pozaunijnymi członkami grupy kapitałowej objętymi BCC a żadnym z europejskich członków grupy. BCC wymagają zatwierdzenia przez organ nadzorczy ochron danych z terenu UE, a do tego zatwierdzenia potrzebna jest akceptacja organów nadzorczych wszystkich państw członkowskich, dane osobowe z terenu których mają być objęte BCC. BCC mogą dotyczyć pewnej kategorii osób lub danych – np. danych pracowniczych.

Cisco widnieje na liście firm, których wiążące reguły korporacyjne zostały zatwierdzone przez europejskie organy ochrony danych.[14]. Mimo że Cisco podaje bezpośredni link, gdzie można pobrać kopię takich zatwierdzonych wiążących reguł korporacyjnych, to jednak link nie odwołuje się do poprawnego dokumentu (link nie działa). W związku z tym nie jesteśmy w stanie zweryfikować w jakim zakresie „BCRy" wiążą Cisco. Nie wpływa to jednak ujemnie na ogólny wynik oceny, skoro Cisco również zobowiązało się do stosowania Tarczy Prywatności oraz zawiera SCC (standardowe klauzule umowne) wraz z umową przetwarzania danych. Sam fakt przejścia przez Cisco „drogi krzyżowej" procedury zatwierdzania wiążących reguł korporacyjnych wskazuje na dużą świadomość ochrony danych po stronie Cisco i determinację. Procedura zatwierdzania BCRów jest zazwyczaj niezwykle żmudna i czasochłonna.

[13] https://www.cisco.com/c/en/us/about/trust-center/customer-data-privacy-policy.html
[14] https://iapp.org/media/pdf/resource_center/eubcrprocedureclosed.pdf

Bezpieczeństwo danych

Wymogi prawne

Radcy mają obowiązek zapewnić odpowiednie bezpieczeństwo przetwarzanych danych osobowych, w tym poufność danych. Obowiązek zapewnienia bezpieczeństwa wynika w szczególności z następujących przepisów:

art. 5 ust. 1 lit. f RODO

> *Dane osobowe muszą być (…) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").*

art. 32 ust. 1 i 2 RODO

> *1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu, w tym między innymi w stosownym przypadku:*
>
> *a) pseudonimizację i szyfrowanie danych osobowych;*
> *b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;*
> *c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;*
> *d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.*
>
> *2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.*

> *art. 3 ust. 3 ustawy o radcach prawnych (wraz z odpowiadającym mu art. 15 Kodeksu etyki radcy prawnego)*
>
> *Radca prawny jest obowiązany zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzieleniem pomocy prawnej.*

art. 23 Kodeksu etyki radcy prawnego

> *Radca prawny obowiązany jest zabezpieczyć przed niepowołanym ujawnieniem wszelkie informacje objęte tajemnicą zawodową, niezależnie od ich formy i sposobu utrwalenia. Dokumenty i nośniki zawierające informacje poufne należy przechowywać w sposób chroniący je przed zniszczeniem, zniekształceniem lub zaginięciem. Dokumenty i nośniki przechowywane w formie elektronicznej powinny być objęte odpowiednią kontrolą dostępu oraz zabezpieczeniem systemu przed zakłóceniem działania, uzyskaniem nieuprawnionego dostępu lub utratą danych. Radca prawny powinien kontrolować dostęp osób współpracujących do takich dokumentów i nośników.*

Stan wiedzy technicznej

Ustalając, czy usługi wideokonferencyjne oferują poziom bezpieczeństwa odpowiedni do ryzyka ich wykorzystania, można wziąć pod uwagę następujące źródła wiedzy o cyberbezpieczeństwie:

1. Wytyczne i normy uznanych organów, instytutów i organizacji, takich jak NASK, ENISA, NIST, ISACA, ISO czy NCSC, wyznaczające aktualne standardy w zakresie bezpieczeństwa informacji, a także określająca zagrożenia oraz podatności[15].Także brytyjska agencja rządowa – National Cyber Security Centre (NCSC) 16 stycznia 2020 roku wydała wytyczne mające na celu pomoc w ocenie bezpieczeństwa oferowanych na rynku usług komunikacji audio, wideo oraz tekstowej. Aktualny i wyczerpujący zestaw środków zabezpieczenia danych został opisany przez niemiecką agencję Teletrust[16] we współpracy z ENISA[17]
2. Dokumentację i deklaracje dostawców na temat usługi – w celu weryfikacji spełniania przez usługi ustalonych standardów,
3. Informacje i doniesienia medialne oraz publikacje naukowe na temat bezpieczeństwa, incydentów, podatności związanych z daną usługą lub rozwiązaniami,
4. Wiarygodność dostawcy, w tym certyfikaty, którymi się legitymuje.

Podstawowe środki bezpieczeństwa. Biorąc pod uwagę sposób planowanego wykorzystania usług, na podstawie powyżej wskazanych źródeł można odtworzyć listę podstawowych środków bezpieczeństwa, jakie usługa służąca do elektronicznej komunikacji video, audio oraz tekstowej powinna zapewniać, którą prezentujemy poniżej. Dla przejrzystości, przy każdym ze środków podajemy odniesienie do odpowiednich postanowień normy PN-EN ISO/IEC 27001:2017-06.

1. Zabezpieczenia przesyłanych i przechowywanych danych, w tym szyfrowanie (A.10.1)
2. Uwierzytelnianie użytkowników (A.9.4.1, A.9.4.2.)
3. Zarządzanie dostępami i uprawnieniami użytkowników oraz administratorów (A.9.2.)
4. Zarządzanie funkcjonalnościami usługi (A.12.1)
5. Ciągłość usługi (A.17.1).

Środki bezpieczeństwa stosowane. Usługi zapewniają rozwiązania techniczne i organizacyjne mające na celu zapewnienie środków bezpieczeństwa, o których mowa w akapicie powyżej. Są one jednak różne w zależności od usługi, a co za tym idzie inna może być ocena zapewnianego przez te usługi poziomu bezpieczeństwa.

Zabezpieczenie przesyłanych i przechowywanych danych

Poufność. Podstawowym środkiem technicznym zapewniającym poufność informacji cyfrowych jest szyfrowanie. Stosowane są różne metody szyfrowania danych w trakcie ich przesyłu (*encryption in transit*) a także w trakcie ich przechowywania (*encryption at rest*).

[15] Przykładowo: Wytyczne NCSC w zakresie oceny bezpieczeństwa usług komunikacji https://www.ncsc.gov.uk/guidance/secure-communication-principles-alpha-release, norma ISO/IEC 27001:2017, NIST Special Publication 800-53 https://nvd.nist.gov/800-53

[16] https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

[17] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

W praktyce niewykonalne natomiast jest otwieranie plików przez aplikacje bez odszyfrowywania plików (np. praca na dokumencie Word wymaga odszyfrowania pliku tekstowego, np. docx)[18].

W przypadku szyfrowania danych w przesyle istotne jest pomiędzy którymi dwoma punktami przesyła się informacje zaszyfrowane. Szyfrowanie na pełnej drodze między nadawcą a odbiorcą komunikacji nazywamy szyfrowaniem *end-to-end*.

Teams

Teams zapewnia szyfrowanie przesyłanych danych w tym audio i video *in transit* oraz *at rest* za pomocą protokołów TLS, MTLS oraz SRTP.

Teams nie zapewnia szyfrowania end-to-end (e2e) pomiędzy uczestnikami spotkania. Komunikacja szyfrowana jest w drodze pomiędzy uczestnikiem spotkania a Microsoft, następnie zostaje odszyfrowywana w ramach infrastruktury Microsoft 365 i ponownie zaszyfrowywana po przekierowaniu do pozostałych uczestników (adresatów komunikacji).

Brak *end-to-end encryption* to jest szyfrowania, w którym także dostawca usługi nie jest w stanie odszyfrować przesyłanych danych, oznacza, że dostawca może, choć nie musi mieć, dostęp do przesyłanych danych. Oznacza to, że Microsoft ma techniczną możliwość zapoznania się z treścią komunikacji uczestników spotkania Teams.

Nie oznacza to, że brak e2e jest automatycznie niebezpieczny, otwiera jednak ekspozycję na dodatkowe ryzyka po stronie dostawcy. Microsoft zobowiązany jest jednak do zachowania poufności.

Jeżeli jednak dostawca właściwie wewnętrznie zarządza bezpieczeństwem informacji, w szczególności, ma prawidłowo zorganizowaną kontrolę dostępu i uprawnień uprzywilejowanych, wtedy nie powinno dojść do ewentualnego nieuprawnionego dostępu do naszych informacji wymienianych podczas wideokonferencji. Zgodnie ze znanymi nam wcześniej oświadczeniami Microsoft, dostęp do treści danych klienta Microsoft Teams wymagałby wcześniejszego poinformowania klienta a także procedury nadania i akceptacji takich czasowych uprawnień w ramach infrastruktury Microsoft[19].

Przy tym, realne ryzyko, że pracownik dostawcy usługi będzie chciał podsłuchiwać akurat naszą polską komunikację i to w czasie rzeczywistym jest, oceniając realnie, pomijalne.

Zoom 5.0

Zoom 5.0 zapewnia szyfrowanie komunikacji za pomocą 256-bitowego protokołu szyfrującego TLS (*Transport Layer Security*) oraz także 256-bitowego AES (*Advanced Encryption Security*).

Zoom od 30 maja wymusza pełne szyfrowanie e2e pomiędzy nadawcą i adresatami komunikacji. Powinno to zapewniać najwyższy poziom poufności danych w przesyle – także pracownicy Zoom nie mogą mieć dostępu do przesyłanych danych, które zostały zaszyfrowane w tym trybie.

[18] W teorii takie działanie jest możliwe przy zastosowaniu tzw. szyfrowania homomorficznego. Nikt na razie jednak nie wymyślił sposobu korzystania z tej metody szyfrowania bez konieczności przesyłu danych w ilości drastycznie przekraczającej obecne możliwości sieci.

[19] Przygotowując tę opinię nie natrafiliśmy ponownie na opisane tu informacje o pragmatykach bezpieczeństwa Microsoft. Znane są nam one z wcześniejszych analiz. Zapewne zapytanie skierowane bezpośrednio do Microsoft pozwoliłoby jednoznacznie potwierdzić ich aktualność.

Webex

Webex zapewnia szyfrowanie komunikacji za pomocą 128-bitowego[20] lub 256-bitowego protokołu TLS. Zweryfikowane przez nas źródła nie wyjaśniają, w jakim zakresie które szyfrowanie jest stosowane przez Webex.

Webex domyślnie nie zapewnia szyfrowania e2e. Użytkownicy biznesowi mogą włączyć tę opcję ale wtedy, jak rozumiemy, nie będzie działać przesył wideo, czyli platforma Cisco Webex Video[21].

Uwierzytelnianie użytkowników

Bezpieczna usługa powinna zapewniać proces uwierzytelniania użytkowników, tzn. potwierdzania ich tożsamości, w oparciu o wiarygodne narzędzia. Przeciwieństwem będzie tutaj aplikacja otwarta, która nie wymaga uwierzytelniania użytkowników. Podstawowym narzędziem uwierzytelnienia są login oraz indywidualne hasło użytkownika. Standardem jednak staje się uwierzytelnianie dwuskładnikowe (2FA = *two factor authentication*, MFA = *multi factor authentication*, SCA = *strong customer authentication*).

MS Teams

MS Teams zapewnia proces uwierzytelniania użytkowników poprzez sam login i hasło (*single factor authentication* - SFA) lub z użyciem dodatkowego składnika – np. PIN-u. telefonu, odcisku palca (*multi factor authentication* - MFA). Uwierzytelnienie chroni przed nieuprawnionym dostępem do konta zarejestrowanego użytkownika, np. w przypadku fizycznego przejęcia sprzętu. MFA jest oczywiście bezpieczniejszą metodą uwierzytelniania. Dostawca udostępnia obie z nich, a decyzja o uruchomieniu opcji MFA zależna jest od klienta usługi.

Proces uwierzytelnienia następuje poprzez usługę dostawcy – *Azure Active Directory*.

Zoom

Zoom zapewnia proces uwierzytelniania użytkowników za pomocą loginu i hasła. Umożliwia także zaawansowane uwierzytelnianie za pomocą *single sign-on* czyli pojedynczego uwierzytelnienia zapewniającego dostęp do wielu usług zintegrowanego z usługą zewnętrznego dostawcy tożsamości np. z *Azure Active Directory*. Zoom umożliwia na dzisiaj uwierzytelnienie dwuskładnikowe tylko przez przeglądarkowy dostęp do usługi[22] (a nie w aplikacji).

Do niedawna Zoom umożliwiał domyślnie organizację i zapraszanie na spotkania wyłącznie linkiem (czyli wiedzą o wirtualnej lokalizacji spotkania). Obecnie domyślnie wymaga też hasła.

Webex

Webex zapewnia uwierzytelnianie użytkowników za pomocą SFA opartego na haśle użytkownika. Oferuje także możliwość wdrożenia *single sign-on* opartego na zewnętrznym dostawcy tożsamości. W przypadku *single sign on* możliwe jest wdrożenia 2FA.

Dlaczego uwierzytelnienie jednoskładnikowe wystarczy

W naszej ocenie jednoskładnikowe uwierzytelnienie jest wystarczające dla usług wideokonferencyjnych, ze względu na ich naturę.

---

[20] Zgodnie z tabelką na stronie 42. https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/Cisco-Webex-Apps-Security-White-Paper.pdf

[21] https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf pkt 7 na końcu

[22] https://support.zoom.us/hc/en-us/articles/360038247071-Setting-up-and-using-two-factor-authentication

Podczas wideokonferencji zasadniczo widzimy i słyszymy uczestników, zwykle też ich znamy, a także zaproszenia na ogół wysyłamy na ich emaile. Powoduje to, że w praktyce stosujemy nie tylko metodę uwierzytelnienia login/hasło (wiedza) ale także metodę coś masz (token, którym w tym przypadku jest email lub telefon) oraz metodę quasi-biometryczną – słyszę i widzę, z kim rozmawiam.

Natomiast w przypadku większych spotkań, gdy nie mamy możliwości widzieć uczestników (choćby z powodu obciążenia łącza) a czasem też ich nie słyszymy i nie znamy (webinarium), nie przekazujemy danych poufnych.

Zarządzanie dostępami i uprawnieniami użytkowników oraz administratorów

Klient usługi powinien mieć możliwość samodzielnego zarządzania dostępami użytkowników oraz zakresem ich uprawnień.

Teams

MS Teams pozwala klientowi usługi ustanawiać użytkowników o zróżnicowanych uprawnieniach, w tym administratorów. Utworzeni użytkownicy rozpoznawani są dalej jako członkowie organizacji klienta usługi, np. kancelarii.

Zoom

W ramach konta klienta usługi Zoom umożliwia ustanawianie użytkowników o różnych poziomach uprawnień w tym administratorów i członków. Zoom pozwala także przypisać do konta właściciela domenę lub domeny. Jest to istotne z punktu widzenia zarządzania spotkaniami, gdyż możliwe jest ograniczenie uczestników wyłącznie do tych posługujących się zaakceptowaną domeną.

Webex

Webex Cisco umożliwia klientowi usługi ustanawianie użytkowników o różnych poziomach uprawnień, w tym uczestników najniższego poziomu, gospodarzy sesji oraz administratorów. W organizowanych spotkaniach możliwy jest udział uczestników spoza listy użytkowników właściciela, ale jednocześnie spotkania można ograniczyć wyłącznie do zarejestrowanych użytkowników.

Zarządzanie funkcjonalnościami

W celu efektywnego zapewnienia bezpieczeństwa danych przetwarzanych w usłudze kluczowe jest istnienie oraz właściwie wykorzystanie funkcjonalności pozwalających zarządzać dostępami uczestników do konkretnych sesji oraz ich uprawnieniami w ramach sesji. Zapobiega to incydentom związanym z dołączeniem do spotkania przez nieuprawnione osoby trzecie.

Teams

W ramach Teams można modyfikować kategorie użytkowników, którzy będą mogli dołączyć do spotkania bezpośrednio (użytkownicy w ramach organizacji) lub pośrednio poprzez „poczekalnię", po ich zaakceptowaniu (np. użytkownicy innych akceptowanych organizacji czy użytkownicy anonimowi). Istnieje opcja całkowitego wyłączenia możliwości dołączania do spotkania użytkowników anonimowych, tj. nieuwierzytelnionych w Teams poprzez *Azure Active Directory*.

Teams umożliwia organizację tzw. *structured meetings*, w ramach, których użytkownicy pełniący rolę prezenterów spotkania posiadają znacznie szerszy zakres uprawnień od pozostałych uczestników. Decydują oni o wpuszczeniu uczestników z poczekalni na spotkanie,

mogą usuwać uczestników, decydować o nagraniu lub przerwaniu nagrania spotkania, udostępniać pliki, podczas gdy rola pozostałych użytkowników sprowadza się jedynie do uczestniczenia w spotkaniu za pośrednictwem audio, video oraz chatu. Usługa wyróżnia łącznie trzy rodzaje użytkowników uczestniczących w spotkaniach – organizator (członek organizacji „właściciela" spotkania) będący jednocześnie prezenterem, który decyduje o ustawieniach spotkania, prezenterzy wyznaczeni przez organizatora oraz uczestnicy.

Usługa posiada funkcjonalności pozwalające organizatorowi spotkań zarządzać dostępem uczestników oraz przebiegiem spotkania.

Zoom

Spotkaniom organizowanym w Zoom nadawany jest identyfikator dystrybuowany do uczestników przez organizatora, pozwalający dołączyć do spotkania. Obecnie, w wersji Zoom 5.0., domyślnie generowane jest też hasło niezbędne do dołączenia. Istnieje także możliwość ograniczenia uczestników, którzy mogą dołączyć do spotkania poprzez: (i) uprzednią, obowiązkową rejestrację wymagającą zatwierdzenia przez organizatora lub (ii) ograniczenie możliwości uczestniczenia w spotkaniu wyłącznie dla użytkowników określonej domeny.

Zoom także oferuje funkcję „poczekalni". W przypadku jej włączenia, zanim uczestnik dołączy do spotkania, podlega akceptacji organizatora. W każdej chwili organizator może usunąć uczestnika ze spotkania lub też uruchomić opcję blokady, zabezpieczającą przed dołączeniem kolejnych uczestników. Ma także możliwość zarządzania uprawnieniami uczestników takimi jak korzystanie z chatu czy udostępniania ekranu.

Webex

Dostęp do konkretnych spotkań w Webex można zabezpieczyć hasłem. Dotyczy to także nagrań ze spotkań. Możliwe jest także włączenie wymogu uwierzytelnienia. Wówczas nieuwierzytelnieni użytkownicy nie będą mogli dołączyć.

Interesującym rozwiązaniem oferowanym przez usługę wydaje się opcja Personal Room (oferowana także przez Zoom). Organizator dysponujący tą usługą posiada własny adres URL miejsca spotkań. W ramach Personal Room dostępna jest opcja poczekalni – użytkownicy nie mogą dołączyć do spotkania bez akceptacji gospodarza, a także blokowania możliwości dołączania do spotkania.

także istnieje możliwość włączenia lub wyłączenia możliwości przesyłu danych, nagrywania czy udostępniania ekranu. Kontrolę przebiegu spotkań zapewnia podział również ról i uprawnień. Administrator może decydować o pewnych z góry określonych ustawieniach bezpieczeństwa. Pozostali użytkownicy mogą poruszać się w ramach wyznaczonych przez niego ram. W szczególności chodzi tu o organizatora oraz prezentera na spotkaniu.

Medialne informacje o podatnościach

W marcu i kwietniu 2020 r., w wyniku zwiększonego wykorzystania usługi Zoom do pracy zdalnej odkryto a następnie upubliczniono informacje o licznych podatnościach i lukach bezpieczeństwa, pozwalających na nieuprawniony dostęp do przetwarzanych w niej danych. Chodziło m.in. o brak zabezpieczeń przed dołączaniem do spotkań osób trzecich, czy posługiwanie się przez dostawcę niedookreśloną definicją szyfrowania *end-to-end*, a w konsekwencji mogącą wprowadzać w błąd deklaracją w tym zakresie.

Dostawca zareagował szybko, ogłaszając ekspresowy plan poprawy bezpieczeństwa. Już pod koniec kwietnia 2020 r. ukazała się nowa, ulepszona wersja Zoom 5.0, której to funkcjonalności poddane zostały analizie powyżej. Wydaje się, że na wysokim poziomie, w aktualnej wersji Zoom nie odbiega poziomem bezpieczeństwa od Teams i Webex a w zakresie szyfrowania end-to-end nawet przewyższa konkurencję.

Co do Microsoft Teams – informowano niedawno o wycieku nagrań rozmów wsparcia Microsoft 365 z użytkownikami.

Co do Webex – jak wspominaliśmy, w 2019 Cisco przypadkiem skasowało cały Webex i kilka dni pracowało nad jego odtworzeniem.

Certyfikacje bezpieczeństwa

Miarodajne dla oceny bezpieczeństwa i wiarygodności dostawcy oraz usługi mogą być także posiadane przez te podmioty uznane i rozpoznawalne certyfikaty.

MS Teams

Microsoft udostępnia szereg audytów i certyfikatów niezależnych audytorów, w tym: ISO 27001, 270018, SOC 1, SOC 2[23].

Zoom

Zoom deklaruje, że posiada certyfikaty zgodności m.in. SOC 2 oraz FedRAMP[24]. Jak rozumiemy, na razie nie posiada innych certyfikatów, w tym w szczególności ISO 27xxx

Webex

Webex deklaruje dla usługi m.in. zgodność z SOC 2 oraz certyfikację 27001[25].

Podsumowanie. Zewnętrzne audyty i certyfikacje podnoszą wiarygodność dostawcy i jego usługi. Tu przoduje Microsoft zaś Zoom pozostaje w tyle. Jednak głównym weryfikatorem wiarygodności obecnie pozostaje rynek i informacje rynkowe. Jak na razie nie dotarły do nas informacje o tym, aby z przyczyn podatności Zoom 5.0, podmioty nieuprawnione przechwyciły informacje poufne.

Podsumowanie. Zgodnie z dokumentacją, informacjami i deklaracjami dostawców na temat usług, wszystkie usługi wydają się zapewniać obecnie właściwy standard bezpieczeństwa obejmujący szyfrowanie komunikacji, możliwość zarządzania rolami i uprawnieniami użytkowników oraz efektywnego zarządzania dostępami do organizowanych spotkań. Microsoft ma przewagę szeregu zewnętrznych audytów a Zoom przewagę szyfrowania end-to-end.

Analiza ryzyka

Zgodnie z art. 32 RODO, cytowanym powyżej, ocenę odpowiedniości środków bezpieczeństwa należałoby zacząć od oceny ryzyka przetwarzania danych.

Analizę ryzyka korzystania z usług wideokonferencyjnych naszkicowaną w niniejszej opinii przeprowadziliśmy zgodnie z zasadami naszej autorskiej metodyki uproszczonej analizy ryzyka przetwarzania, opisanymi w książce **„Ochrona danych osobowych. Przewodnik po ustawie i rodo z wzorami”**[26]**(**s. 801 i następne)**,** będącej drugim wydaniem popularnego „RODO Przewodnik ze wzorami”. Moduł uproszczonej analizy ryzyka dostępny jest w usłudze zarządzania zgodnością ochrony danych osobowych **Good Data Protection Standard (gdpstandard.com)**.

Atrybuty bezpieczeństwa. Aby zapewnić bezpieczeństwo informacji, w praktyce muszą być spełnione trzy zasadnicze atrybuty bezpieczeństwa poufność, integralność, dostępność – każdy na poziomie odpowiednim do ryzyk generowanych przez przetwarzanie danych.

[23] https://servicetrust.microsoft.com/ViewPage/MSComplianceGuide
[24] https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf
[25] https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf, s. 11
[26] https://www.profinfo.pl/sklep/ochrona-danych-osobowych-przewodnik-po-ustawie-i-rodo-ze-wzorami,90625.html

Integralność. Zgodnie z założeniami uproszczonej analizy ryzyka, aspekt integralności danych klasyfikujemy jako element poufności lub dostępności danych, w zależności od kontekstu potencjalnego zdarzenia operacyjnego. Celowa podmiana danych lub zakłócanie komunikacji (np. tzw. Zoombombing) będą efektem naruszenia poufności – przechwycenia danych uwierzytelniających lub podatności umożliwiającej nieautoryzowane dołączenie do spotkania. Pogorszenie jakości danych – czyli pogorszenie komunikacji samo w sobie nie rodzi szczególnych ryzyk, gdyż zwykle dostępne są inne kanały komunikacji zdalnej: email, czat, telefon, komunikatory. Wszystkie skądinąd obecnie bazują na dostępności internetu.

Dostępność danych. Niedostępność danych, czyli niemożność przeprowadzenia wideokonferencji, nie rodzi, w naszej ocenie, szczególnego ryzyka, gdyż albo będzie substytuowana możliwością skorzystania z innego kanału komunikacji, albo będzie niemożliwa do uniknięcia. W razie awarii usługi wideokonferencyjnej można skorzystać z innej takiej usługi lub zestawić zwykłą telekonferencję, można też komunikować się emailem.

Tak więc, poniższa analiza koncentruje się na zapewnieniu poufności wideokonferencji.

Poufność. Powaga wycieku danych podczas wideokonferencji z klientem jest wyższa niż powaga wycieku danych wideokonferencji posiedzenia organu samorządu radcowskiego. Sprawy samorządowe mają z natury mniejszy poziom poufności. Więcej osób w nich uczestniczy oraz nie powinno się utrzymywać ich w poufności względem członków samorządu. Stąd środki ochrony danych adekwatne dla wideorozmowy z klientem (jako obarczonej większym ryzykiem poufności) będą zapewne też adekwatne dla posiedzenia organu samorządu.

Ryzyko cichego włamania. Dotychczas brak doniesień o tym, aby możliwy był „cichy dostęp" do spotkań w którejkolwiek z usług. Tzn. każdy gość – nawet nieproszony – jest widoczny. Stąd spotkania w mniejszym gronie wymagają niższego poziomu uwierzytelnienia (dlatego Zoom dotychczas umożliwiał domyślne dołączanie do spotkania wyłącznie za pomocą linka).

Rozpoznawalność uczestników. Jak wspominaliśmy, wdrożenie uwierzytelniania wielopoziomowego jak MFA (ang. *multi-factor authentication)* nie zawsze jest konieczne. Weryfikacja tożsamości przy mniejszych spotkaniach następuje na ogół głosowo i wizualnie. Tak więc, sile uwierzytelnienie uczestników spotkania jest w pewnym sensie wbudowane w medium[27]. Zatem realne ryzyko wycieku danych w trakcie małego spotkania wskutek dołączenia nieproszonego gościa jest bardzo niskie – uczestnicy spotkania powinni być w stanie wychwycić w czasie rzeczywistym dołączenie osoby nieproszonej, szczególnie gdy włączona jest transmisja wideo i uczestnicy spotkania się znają.

Ryzyko wycieku danych. Ryzyko wycieku danych wskutek przejęcia danych uwierzytelniających (credentials) również wydaje się niskie, a co więcej, wymagałoby zasadniczo tzw. ataku targetowanego, to znaczy ktoś celowo chciałby nas podsłuchiwać. Jednak i w tej sytuacji uczestnicy spotkania zobaczą, że dołącza się kolejny użytkownik z tą samą tożsamością, co jeden z nich.

Ogólne ryzyko poufności wideokonferencji. W naszej ocenie, ogólnie ryzyko korzystania z usług wideokonferencyjnych jest niskie, niższe od ryzyka korzystania z rozmów telefonicznych.

Każda z przeanalizowanych przez nas usług wymaga uwierzytelnienia za pomocą hasła. Umożliwiają one też w pewnym zakresie ustanowienie uwierzytelnienia dwuskładnikowego, choć potrzeba takiego uwierzytelnienia jest wątpliwa z wyłuszczonych względów.

Dotychczas problemy pojawiały się raczej w związku z tzw. zoombombingiem, czyli paraliżowaniem spotkań przez publikowanie niestosownych treści przez jednego z uczestników. Taki problem wśród radców wydaje się mało prawdopodobny. A gdyby nawet wystąpił, można po prostu podnieść poziom wymogów uwierzytelnienia i ustalić nowe spotkanie.

[27] – czyli paradoksalnie mamy MFA.

Wydaje się, że praktycznie każda usługa wideokonferencyjna, która funkcjonuje na rynku i oferuje ją odpowiednio duży dostawca (taki, któremu zależy na utrzymaniu reputacji rynkowej), będzie zapewniała bezpieczeństwo odpowiednie do potrzeb radców.

Wiarygodność dostawcy

Art. 28 RODO

> *1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora,* ***korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje*** *wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.*
>
> *3. Przetwarzanie przez podmiot przetwarzający odbywa s****ię na podstawie umowy*** *lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:*

Powierzenie przetwarzania. Zweryfikowaliśmy pozytywnie zgodność zobowiązań Microsoft, Zoom i Cisco z wymogami art. 28 RODO, w ramach oceny umowy powierzenia przetwarzania.

Transfer danych. Zweryfikowaliśmy zakres transferu danych osobowych poza EOG przez dostawców i prawne podstawy legitymizujące ten transfer.

Bezpieczeństwo. Zweryfikowaliśmy informacje o bezpieczeństwie usług jak też i o ocenie ryzyka samego korzystania z nich, dochodząc do wniosku, że zapewniają one odpowiednie bezpieczeństwo danych.

Podatności. Zgłaszane są podatności każdej z omawianych usług. Najczęściej zgłaszane były różnego typu możliwości nieautoryzowanego dołączania do spotkań. Dostawcy szybko na te zgłoszenia reagują.

Wycieki danych i inne naruszenia ochrony danych. Nie wiadomo nam o bezpośrednich wyciekach danych z żadnej z omawianych usług. Jak wspominaliśmy w 2019 usługa Webex została przypadkowo skasowana, wskutek błędu ludzkiego, co umożliwiło wadliwe określenie poziomów uprawnień administratorów. Lekcja zapewne została wyciągnięta. Z Microsoft 365 wyciekły niedawno nagrania rozmów z użytkownikami. To również zostało obsłużone, oraz tego typu wyciek raczej nie grozi ujawnieniem informacji poufnych danej organizacji. Zoom w wersjach poprzedzających 5.0 znany był z zoombombingu, czyli raczej z niewystarczającego poziomu domyślnych zabezpieczeń niż z czystych podatności.

Wiarygodność rynkowa. Wiarygodność Microsoft i Cisco wspierana jest przez wieloletnią historię tych firm. Zoom jest organizacją relatywnie świeżą (2011). Ostatnio, w związku z potężnym sukcesem rynkowym Zoom jest w centrum światowej uwagi i zarzucane mu są różnego typu podatności (ale nie wycieki) i niezgodności (handel danymi z Facebookiem). Jednak Zoom błyskawicznie reaguje na tego typu spostrzeżenia rynkowe i dostosowuje swoje praktyki (zrezygnował z udostępniania danych Facebookowi), w wersji 5.0. wprowadził szyfrowanie end2end skuteczne także względem „siebie". Stąd można zasadnie przypuszczać, że Zoom jest już usługą o odpowiednim poziomie wiarygodności i wiarygodność ta będzie rosła – wobec światowego zainteresowania.

Podsumowanie. Każdy z omawianych dostawców jest wiarygodny, a usługi przez nich oferowane zapewniają wiarygodne gwarancje bezpieczeństwa i legalności przetwarzania danych osobowych i nieosobowych**.**

Obowiązek informacyjny

Zgodnie z art. 13 RODO administrator danych powinien informować osobę, której dane dotyczą, o szeregu okoliczności dotyczących przetwarzania jej danych osobowych. Organizator spotkania wirtualnego powinien spełnić ten obowiązek. Radcy powinni więc opracować treść obowiązku informacyjnego odpowiednią względem usługi, z której będą korzystać (zmienne to na przykład stanowisko dostawcy co do administrowania danymi technicznymi itp., zakres eksportu danych) i prezentować te informacje wraz z informacją o regulaminie usługi (kiedy przedstawienie regulaminu jest konieczne).

Przykładowo, radca prawny do zaproszenia na spotkanie może umieścić następującą informacje:

Administratorem Państwa danych osobowych jest „Zenon Xenon i Wspólnicy sp.k." info@zxenon.pl. Wasze dane osobowe będę przetwarzane w celu umożliwienia nam wzajemnej komunikacji w celu, dla którego zorganizowaliśmy a Wy dołączyliście do naszego wirtualnego spotkania, czyli w celu realizacji naszego i Waszego uzasadnionego interesu we wzajemnej komunikacji (art. 6 ust. 1 lit. f RODO).

Jeżeli będziemy chcieli zarejestrować nasze spotkanie, poinformujemy Was o tym.

Dla MS Teams: Naszym dostawcą usługi wideokonferencji jest Microsoft, z którym mamy zawartą umowę przetwarzania danych. Nasza komunikacja jest szyfrowana w standardzie TLS 1.2. 256 bit na odcinku uczestnik – Microsoft i Microsoft – uczestnik. Jeżeli nasze wirtualne spotkanie było nagrywane, wtedy treść komunikacji jest przechowywana w UE. Dane telemetryczne i dane o uczestnikach są przetwarzane centralnie w USA przez Microsoft Inc. jako administratora tych danych. Microsoft Inc. zapewnia zgodność z RODO w ramach uczestnictwa w programie Privacy Shield / Tarcza Prywatności.

Dla Zoom. Naszym dostawcą usługi wideokonferencji jest Zoom Video Communication Inc. (Zoom), z którym mamy zawartą umowę przetwarzania danych wraz z tzw. standardowymi klauzulami umownymi. Nasza komunikacja jest szyfrowana w standardzie TLS 256 bit na całej drodze uczestnik – uczestnik (szyfrowanie end-to-end) i nawet Zoom nie ma dostępu do naszej komunikacji. Jeżeli nasze wirtualne spotkanie było nagrywane, wtedy treść komunikacji jest przechowywana w UE. Zoom również zapewnia, że nie ma dostępu do nagranych spotkań, gdyż dane „w spoczynku" też są szyfrowane. Zoom przesyła do USA dane telemetryczne (czyli np. o tym skąd się łączysz, ile danych przesyłasz, jakie komendy wydajesz usłudze) i podstawowe dane uczestnika (te, które wprowadziłaś/eś sam/a do Zoom rejestrując się na spotkanie). Zoom zapewnia zgodność z RODO takiego transferu danych w ramach uczestnictwa w programie Privacy Shield oraz przez zawarcie z nami tzw. standardowych klauzul umownych zaakceptowanych przez Komisję Europejską.

Dla Webex. Naszym dostawcą usługi wideokonferencji jest Cisco Inc. (Cisco), z którym mamy zawartą umowę przetwarzania danych wraz z tzw. standardowymi klauzulami umownymi. Nasza komunikacja jest szyfrowana w standardzie TLS 1.2. 256 bit na odcinku uczestnik – Cisco i Cisco – uczestnik. Jeżeli nasze wirtualne spotkanie było nagrywane, wtedy treść komunikacji jest przechowywana w UE. Cisco przesyła do USA dane telemetryczne (czyli np. o tym skąd się łączysz, ile danych przesyłasz, jakie komendy wydajesz usłudze) i podstawowe dane uczestnika (te, które wprowadziłaś/eś sam/a do Webex rejestrując się na spotkanie). Cisco zapewnia zgodność z RODO takiego transferu danych w ramach uczestnictwa w programie Privacy Shield oraz przez zawarcie z nami tzw. standardowych klauzul umownych zaakceptowanych przez Komisję Europejską.

Inne. Więcej informacji dotyczących przetwarzania Twoich danych osobowych możesz znaleźć w naszej Polityce Prywatności dostępnej na naszej stronie internetowej tu: zxenon.pl/prywatnosc lub przez bezpośredni kontakt z nami pod adresem e-mail rodo@zxenon.pl

Wynik analizy

Przeprowadzona analiza dokumentacji i deklaracji dostawców oraz doniesień rynkowych w zakresie zapewnienia bezpieczeństwa i legalności ochrony danych osobowych oraz obowiązku ochrony informacji objętych tajemnicą radcowską, wskazuje na zgodność wykorzystania analizowanych rozwiązań przez radców prawnych w ramach świadczenia pomocy prawnej, w szczególności komunikacji z klientami oraz organizacji szkoleń, a także na potrzeby pracy organów samorządu radcowskiego.

Istotna pozostaje kwestia odpowiedniej konfiguracji oferowanych funkcji oraz właściwe zarządzanie wewnętrzne tymi usługami – np. dostępami użytkowników. Każda z usług pozostawia klientowi dużą swobodę w tym zakresie. Od spotkań otwartych, umożliwiających dostęp użytkownikom anonimowym, bez uwierzytelnienia, po spotkania prywatne, obwarowane wieloskładnikowym uwierzytelnieniem użytkowników i dostępem ograniczonym dodatkowym hasłem. Natomiast według naszej oceny i naszej analizy ryzyka, domyślne opcje bezpieczeństwa Teams i Zoom są wystarczające. Zoom 5.0 domyślnie generuje hasło i stosuje szyfrowanie e2e. Teams nie generuje hasła domyślnie ale uczestników spoza organizacji umieszcza w poczekalni. Aktualnych ustawień domyślnych Webex nie znamy.

Wskazówki praktyczne

- **Aplikacja desktopowa**. Wskazówka ogólna – warto zainstalować desktopowa wersję aplikacji. Zainstalowana aplikacja na komputerze ułatwia zarządzanie i planowanie spotkań. Uwaga: Zoom umożliwia uwierzytelnianie dwuskładnikowe tylko przy dostępie przez WWW. Tzw. eksperci cyberbezpieczeństwa wskazują to jako pewną słabość. Eksperci na tym poziomie porad nie biorą jednak pod uwagę zwykle wymiaru prawdopodobieństwa błędu ludzkiego – czyli problemów z obsługą. Obsługa aplikacji wideokonferencyjnych jest zwykle bardziej intuicyjna niż obsługa usługi wideokonferencyjnej przez przeglądarkę.
- **Hasłowanie**. W sprawach objętych tajemnicą zawodową i tajemnicą przedsiębiorstwa (np. omawianie kwestii korporacyjnych), spotkanie powinno być chronione hasłem. Przy organizacji webinariów czy szkoleń, również rekomendujemy hasłowanie spotkań. Wprawdzie ryzyko naruszeń przy szkoleniach czy webinariach jest niższe, jednak zawsze istnieje potencjalne ryzyko tzw. „zoombombingu”.
- **Poczekalnia**. Rekomendujemy korzystanie z opcji „poczekalnia”. Jest to ważna funkcja dla organizatora spotkania, aby mógł kontrolować kto dołącza do spotkania.
- **Regulamin**. Należy opracować regulamin korzystania z usługi. Najlepiej taki regulamin udostępnić w zaproszeniu do spotkania (wraz z obowiązkiem informacyjnym). Regulamin jest realnie potrzebny dla większych spotkań. Formalnie regulaminu nie trzeba opracowywać dla spotkań wewnątrz organizacji, ale i dla takich regulacji rekomendujemy opracowanie regulaminu.
- **Zarządzanie udostępnianiem ekranu.** Szczególnie polecane przy organizacji szkoleń i dużych spotkań, gdzie większość uczestników będzie uczestniczyć „biernie” w spotkaniu. Aby ograniczyć ryzyko dzielenia się np. niechcianymi lub nielegalnymi treściami, radca jako organizator powinien zaznaczyć opcję, że tylko organizator (lub wybrane osoby) spotkania mogą udostępniać ekran.
- **Blokowanie spotkania**. Jeżeli jest to możliwe, po dołączeniu do spotkania wszystkich wymaganych użytkowników warto jest włączyć opcję „zablokuj spotkanie”. To taka

funkcji jak „zamknięcie drzwi”. Po zablokowaniu spotkania nikt już nie będzie mógł do spotkania dołączyć.

- **Przypisywanie ról.** W przypadku większych spotkań warto przypisywać role poszczególnym osobom w spotkaniu. Radca jako organizator może przypisać uprawnienie dzielenia się materiałami, czy współdzielenia ekranu dla wszystkich lub dla poszczególnych użytkowników.
- **Monitorowanie doniesień**. Radca powinien monitorować doniesienia o wyciekach i naruszeniach związanych z poszczególnymi usługami. W praktyce oznacza to pozostawianie na tzw. „nasłuchu” np. branżowych mediów społecznościowych (np. grup IODów). Wskazane jest, aby funkcja monitorowania bieżących doniesień o podatnościach, naruszeniach i praktykach została zcentralizowana przez samorząd radcowski, aby zluzować poszczególnych radców.

Głosowanie przez usługę

Każda z analizowanych usług oferuje opcję głosowania, w tym głosowania anonimowego. Głosowanie za pomocą usługi podmiotu trzeciego musi w dużej mierze opierać się o zaufanie do tego podmiotu. Nie przeprowadziliśmy analiz metod organizacji tych głosowań ani metod zapewnienia ich gwarancji. Stąd na razie rekomendowalibyśmy organom samorządu skorzystanie z rynkowych rozwiązań do zdalnego głosowania podczas walnych zgromadzeń, jak na przykład rozwiązanie oferowane przez GPW. Oczywiście deklarujemy gotowość do rozpoznania funkcji głosowania w globalnych aplikacjach.

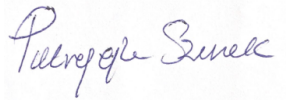
Udział w wideokonferencjach

Opisane w opinii obowiązki nie będą miały zastosowania w przypadku, gdy to nie radca prawny będzie organizatorem spotkań, a będzie jedynie dołączał do spotkań organizowanych przez podmioty trzecie, np. klientów. Nie zwalnia to jednak radcy prawnego z obowiązku dochowania należytej staranności w podejmowaniu komunikacji przy użyciu wiarygodnych i bezpiecznych narzędzi, z uwzględnieniem aspektów ich oceny, opisanych w niniejszej opinii. Chodzi przede wszystkim o zachowanie zdrowej ostrożności, zwłaszcza w przypadku, gdy spotkanie zostanie zorganizowane przy użyciu nieznanych usług lub też jego przebieg sugerował będzie możliwość dostępu do przekazywanych treści przez osoby nieuprawnione.

* * *

Mamy nadzieję, że opinia jest dla Państwa użyteczna, czytelna i adresuje zagadnienia, z którym się do nas Państwo zwrócili. Pozostajemy do Państwa dyspozycji w tej sprawie jak i w każdej innej, z którą zechcą się Państwo do nas zwrócić, w tym w szczególności w sprawach dotyczących zgodności i bezpieczeństwa różnego typu usług chmurowych, oraz dobrych praktyk prawnych dotyczących informatyki i gospodarki cyfrowej.





Maciej Gawroński
radca prawny, CIPP/E

Michał Ćwiakowski

Patrycja Szurmak
aplikantka radcowska

adwokat, certyfikowany auditor wiodący ISO 27001

O autorach

Maciej Gawroński

Radca prawny, Certified International Privacy Professional Europe of International Association of Privacy Professionals (CIPP/E IAPP), partner Gawroński & Partners, współautor systemu Good Data Protection Standard (gdpstandard.com). Redaktor i współautor książek „Guide to the GDPR", bestsellerowego „RODO. Przewodnik ze wzorami", „Ochrona danych osobowych. Przewodnik po RODO i Ustawie z wzorami", „Cloud computing w polskim sektorze finansowym – Regulacje i standardy", autor i współautor wielu innych publikacji z obszaru ochrony danych osobowych, outsourcingu, cloud computingu, przeciwdziałania praniu pieniędzy i innych.

Ekspert Komisji Europejskiej do spraw kontraktów cloud computingowych, konsultant Grupy Roboczej Art. 29 do spraw projektu klauzul umownych Ad hoc "przetwarzający dane w EU do pozaunijnego podprzetwarzającego" (WP214), członek Grupy Roboczej ds. Ochrony Danych przy Ministerstwie Cyfryzacji. Wykłada prawne aspekty cloud computingu i ochrony danych na studiach podyplomowych Szkoły Głównej Handlowej i Uczelni Łazarskiego. Regularnie wyróżniany w międzynarodowych i krajowych rankingach prawniczych jako jeden z wiodących polskich prawników technologii, mediów, telekomunikacji i ochrony danych osobowych.

Mec. Gawroński przez ponad 10 lat odpowiadał za prawne aspekty największego projektu informatycznego w Polsce – wdrożenia systemu ZSI w banku PKO BP.

Mec. Gawroński zajmuje się także sporami. Skutecznie reprezentował klientów w setkach spraw, w tym w sprawach o wartości przekraczającej 10 miliardów złotych.

MICHAŁ ĆWIAKOWSKI

Adwokat, Counsel i Szef Praktyki Regulacji Bankowych i Finansowych Gawroński & Partners

Ekspert regulacji rynku finansowego oraz nowych technologii. Pracował w największych bankach w Polsce, zarówno w obszarze prawnym, jak i ryzyka, oraz wiodących polskich kancelariach prawnych.

Praktyka Mec. Ćwiakowskiego koncentruje się w obszarze IT, AML, usług płatniczych, prawa bankowego, compliance, ładu korporacyjnego, ochrony danych osobowych, cyberbezpieczeństwa oraz nowych technologii. W tych dziedzinach prowadził kompleksowe projekty wdrożenia regulacji oraz audytów powdrożeniowych.

Stały felietonista portalu fintek.pl. Współautor licznych publikacji, między innymi pierwszego przewodnika do nowej ustawy AML – „Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Praktyczny przewodnik" wydanego przez Wolters Kluwer w 2018 roku oraz pozycji „Ograniczanie zatorów płatniczych. Praktyczny przewodnik" Wolters Kluwer 2020.

Członek ORA w Warszawie. Certyfikowany audytor wiodący systemów zarządzania bezpieczeństwem informacji zgodnie z PN-EN ISO/IEC 27001:2017.

PATRYCJA SZURMAK

Aplikantka radcowska, Associate Gawroński & Partners

Patrycja specjalizuje się w obszarze ochrony danych osobowych, nowych technologii, własności intelektualnej, eCommerce oraz telemedycyny. Patrycja zdobywała doświadczenie w międzynarodowej korporacji w dziale prawnym oraz w butikowych polskich kancelariach. W kancelarii Gawroński & Partners od 2017 roku, członek zespołu data protection & IP & IT.

Patrycja bierze udział w złożonych projektach wdrożeniowych oraz audytowych RODO, w tym projektach związanych z identyfikacją i klasyfikacją incydentów bezpieczeństwa danych. Opracowuje umowy wdrożeniowe na systemy IT, w tym z wykorzystaniem usług cloud computingu. Patrycja bierze udział w projektach związanych prawem własności intelektualnej, w tym opracowuje umowy licencyjne, umowy przenoszące prawa własności intelektualnej oraz umowy czy opinie w zakresie korzystania z programów komputerowych. Opracowała szereg regulaminów świadczenia usług drogą elektroniczną w relacjach B2B i B2C.

SZYBKOŚĆ. ZWIĘZŁOŚĆ. TECHNOLOGIA.

Gawroński & Partners to kancelaria prawnicza specjalizująca się w technologii, regulacjach, sporach i prawie karnym gospodarczym.

gppartners.pl
gdpstandard.com
guidetothegdpr.com

linkedin.com/company/gawronskiandpartners
linkedin.com/company/gdpstandard
linkedin/company/guidetothegdpr

facebook.com/gawronskipartners
facebook.com/gooddataprotectionstandard
facebook.com/guidetothegdpr

Autorzy najpoczytniejszej książki o RODO w Polsce, bestsellera 2018 „RODO. Przewodnik ze wzorami„, rekomendowanej przez Prezesa Urzędu Ochrony Danych Osobowych (4 luty 2020), wydanie I po angielsku w 2019 jako „Guide to the GDPR", współautorzy szeregu innych książek i publikacji prawniczych.

Polskie i międzynarodowe rankingi prawnicze od kilkunastu lat wymieniają Macieja Gawrońskiego wśród wiodących ekspertów prawa technologii, mediów, telekomunikacji, ochrony danych osobowych, franszyzy i własności intelektualnej.

Dziękujemy Pani Łucji Mróz-Raynoch za udostępnienie nam ilustracji do "Cyberiady" Stanisława Lema autorstwa Jej ojca wspaniałego Daniela Mroza.

Warszawa, 2020-06-08

Analiza porównawcza ogólnej zgodności oraz niektórych elementów bezpieczeństwa aplikacji do telekonferencji: ZOOM, Microsoft Teams, CISCO Webex

Porównanie wybranych internetowych aplikacji przeznaczonych do prowadzenia spotkań grupowych i wideokonferencji wykonane zostało w celu udzielenia odpowiedzi czy korzystanie z tych aplikacji jest dopuszczalne zgodnie z przepisami o ochronie danych, w tym RODO[28], a także, czy wymienionych dostawców można wstępnie uznać za podmioty, które zapewniają wystarczające gwarancje stosowania przepisów o ochronie danych.

Analiza została wykonana w oparciu o materiały informacyjne i treści regulaminów/umów poszczególnych usług dostępne na stronach www dostawców tych rozwiązań (www.microsoft.com; www.zoom.us; www.cisco.com) oraz na podstawie innych materiałów dostępnych w sieci.

Analiza dotyczy płatnych usług i pakietów dla przedsiębiorstw. Analiza nie dotyczy usług wskazanych dostawców w wersjach bezpłatnych.

Świadczenie usług telekonferencji polega na umożliwieniu użytkownikom tworzenia oraz prowadzenia spotkań z innymi użytkownikami za pośrednictwem sieci Internet. Poza usługą podstawową dostawcy świadczą również usługi dodatkowe, zapewniające odpowiednie funkcjonalności w trakcie spotkania, jak również związane z przechowywaniem danych.

Spotkania mogą być realizowane za pośrednictwem oprogramowania instalowanego na urządzeniu użytkownika, stanowiącego dodatek do przeglądarki internetowej lub też odrębny program komputerowy (Aplikacja dostępowa).

W toku świadczenia usługi dostawcy, co do zasady, będą występować w dwóch rolach:

1) jako administrator danych, działając na podstawie deklaracji zawartych w Zasadach (regulaminie) świadczenia usług oraz Polityce prywatności danego dostawcy – wobec:
    a. danych identyfikacyjnych użytkownika inicjującego spotkanie,
    b. danych identyfikujących użytkownika w przypadku korzystania z Aplikacji dostępowej,
    c. danych telemetrycznych w czasie korzystania z usługi.
2) jako podmiot przetwarzający, działając na podstawie deklaracji zawartych w Zasadach świadczenia usług oraz Umowie powierzenia (DPA) danego dostawcy – wobec:

[28] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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) – zwane „**RODO**”;

a. danych przesyłanych w trakcie spotkania,
b. danych przechowywanych przez użytkowników w infrastrukturze dostawcy (np. dane nagrań).

Ocena kwestii formalnych:

Wszyscy badani dostawcy deklarują zgodność z przepisami o ochronie danych osobowych, w tym RODO, a weryfikacja dokumentów przedstawionych przez tych dostawców potwierdza ich twierdzenia. Jednakże, każdy z dostawców oferuje inny sposób i zasady wykonania warunków umowy. Klienci pragnący skorzystać z usług któregoś z dostawców powinni szczegółowo przeanalizować poszczególne różnice zwracając uwagę na wpływ jaki wywołują one dla jego działalności (zgodnie z podejściem Privacy by Design i Privacy by Default, art. 25 RODO).

Na uwagę zasługują w szczególności różnice związane z prawem umowy, możliwością podejmowania decyzji w zakresie obszaru przechowywania danych, sposobu realizacji obowiązku informowania o nowych podwykonawcach oraz ogólnych zasadach (najczęściej kwotowego) ograniczenia odpowiedzialności dostawcy.

Tabela 1 Porównanie aspektów formalnych (opracowanie własne na podstawie dostępnych materiałów producentów – tylko dla wersji płatnych)

Kryterium/obszar	ZOOM (Zoom VC Inc)	Microsoft Teams	Cisco Webex
Strona umowy	Zoom Video Communications Inc.	Microsoft Ireland Operations Ltd.	Cisco Systems Inc.
Prawo umowy	USA, California	Irlandia[29]	Wlk. Brytania
Czy dane są przekazywane poza UE?	Dane niezbędne da ukształtowania połączenia są przekazywane poza UE.	Dane niezbędne da ukształtowania połączenia są przekazywane poza UE.	Dane niezbędne da ukształtowania połączenia są przekazywane poza UE.
Obszar przetwarzania danych (Treści użytkowników)	Global/Region UE (możliwość ograniczenia obszaru przetwarzania do obszaru UE – tylko dla usług płatnych)	Global/Region UE (możliwość ograniczenia obszaru przetwarzania do obszaru UE – tylko dla usług płatnych)[30]	USA/Global (brak możliwości ograniczenia obszaru przetwarzania danych, ale domyślnie dane przechowywane w regionie użytkowania - UE)[31]
Sposób informowania o podwykonawcach	Ogólna zgoda na podwykonawców Lista (https://zoom.us/subprocessors) Informacja 10 dni przed zaangażowaniem podmiotu[32]	Ogólna zgoda na podwykonawców Lista (dostępna w witrynie) Informacja 14 dni przed zaangażowaniem podmiotu	Ogólna zgoda na podwykonawców Lista dostępna w „Privacy Data Sheet" oraz na żądanie Informacja przed zaangażowaniem podmiotu (bez wskazania czasu)
Sprzeciw administratora	W przypadku sprzeciwu alternatywni dostawcy lub rozwiązanie umowy bez wpływu na opłaty należne dostawcy	W przypadku sprzeciwu możliwość rozwiązania umowy bez ponoszenia kar umownych	W przypadku sprzeciwu możliwość rozwiązania umowy
Czy jest DPA? (Umowa powierzenia zgodnie z art. 28 RODO)	Tak	Tak	Tak
Czy DPA spełnia wymagania art. 28 RODO?	Tak	Tak	Tak
SCC (Standardowe klauzule umowne)	Tak (zawarte w DPA)	Tak (zawarte w DPA)	Tak (zawarte w DPA)
BCR (Wiążące reguły korporacyjne)	-	-	Tak

[29] Brak jednoznacznego wskazania podmiotu świadczącego usługę. Zgodnie z deklaracją na stronie https://www.microsoft.com/pl-pl/servicesagreement/: Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521 Irlandia, Nr w rejestrze VAT IE8256796U.

[30] W przypadku usług online (w tym Office 365, którego częścią jest MS Teams), ograniczenie obszaru przetwarzania danych do wskazanego przez klienta Regionu (może to być UE) polega na tym, że usługa jest co do zasady świadczona za pośrednictwem urządzeń pozostających na terenie UE oraz w taki sposób, aby dane nie były przekazywane do centrów danych poza UE. Jednakże, w szczególnych okolicznościach Microsoft będzie uprawniony do przekazania danych poza UE.

[31] Domyślnie dane są przechowywane w centrum dla danego regionu, jednak bez ograniczenia dla transferu.

[32] Konieczna subskrypcja newslettera informującego o nowych podwykonawcach.

Privacy Shield	Tak	Tak	Tak
Ograniczenie odpowiedzialności	do 12 miesięcy dokonanych opłat	do wpłaconej kwoty za usługi do 5000 USD przy usługach bezpłatnych	do 12 miesięcy dokonanych opłat (ale 1M USD dla DPA)

Ocena niektórych elementów bezpieczeństwa:

Wszyscy badani dostawcy deklarują stosowanie najwyższych środków bezpieczeństwa oraz ochronę poufności komunikacji. Analizując poszczególne obszary oraz zastosowane środki bezpieczeństwa należy brać pod uwagę przede wszystkim okoliczności towarzyszące zastosowaniu poszczególnych środków (np. integracja systemu konferencji z systemami danej organizacji) oraz różnice technologiczne w konstrukcji poszczególnych rozwiązań. Szczególną uwagę należy zwrócić na właściwą konfigurację środowiska oraz domyślnych ustawień dla spotkań (przez wyznaczonego w organizacji administratora systemu telekonferencji / dział IT). Każdy z dostawców oferuje ponadto szereg funkcjonalności zapewniających bezpieczeństwo spotkania i jego uczestników (np. „poczekalnia", czy też uprawnienia organizatora do kontrolowania przebiegu spotkania), których konfiguracja lub zastosowanie pozostaje w rękach organizatora spotkania.

Podsumowując, bezpieczeństwo każdego spotkania uzależnione jest zarówno od parametrów technicznych i konstrukcji rozwiązania danego dostawcy, ale również od właściwej organizacji obszarów pozostających pod kontrolą organizacji oraz organizatorów.

Tabela 2 Porównanie aspektów bezpieczeństwa (opracowanie własne na podstawie dostępnych materiałów producentów – tylko dla wersji płatnych)

Kryterium/obszar	ZOOM (Zoom VC Inc)	Microsoft Teams	Cisco Webex
Ochrona poufności			
Wykorzystanie informacji do innych celów usługodawcy.	Nie (za wyjątkiem danych telemetrycznych)	Nie (za wyjątkiem danych telemetrycznych)	Nie (za wyjątkiem danych telemetrycznych)
Monitorowanie komunikacji	Generalna deklaracja poufności	Generalna deklaracja poufności	Generalna deklaracja poufności
Serwery web	SSL	SSL	SSL
Zabezpieczenie połączenia	TLS 1.2 (256-bit)	TLS 1.2 (256-bit)	TLS 1.2
Zabezpieczenie przekazywanych danych	AES 256-bit	AES-256	AES-256 (UDP AES-128)
Szyfrowanie End-to-End	Tak (domyślnie)	Nie	Tak (jako opcja lub domyślnie)
Przejrzystość dokumentacji	Średnia	Niska	Wysoka
Funkcje użytkownika/ organizatora			
Dostęp do konta	Login i hasło (możliwe SSO[33])	jak w Office 365 (SSO, możliwe wieloskładnikowe uwierzytelnienie)	Login i hasło (możliwe SSO)
Poczekalnia	Tak (konieczność ustawienia przez inicjującego)	Tak	Tak (konieczność ustawienia przez inicjującego)
Hasło do spotkania	Tak (opcja)	opcja dla Anonymous[34]	Tak (opcja)
Nagrywanie spotkań	Na żądanie organizatora	Na żądanie organizatora	Na żądanie organizatora

[33] SSO – Single Sign On – (Wikipedia) możliwość jednorazowego zalogowania się do usługi sieciowej i uzyskania dostępu do wszystkich autoryzowanych zasobów zgodnych z tą usługą. (Tutaj) SSO umożliwia korzystanie z opracowanych uprzednio w organizacji klienta sposobów autoryzacji użytkowników, bez konieczności indywidualnej dodatkowej autoryzacji w usłudze konferencyjnej.

[34] Dostęp bez hasła dla osób z organizacji

Uprzedzenie uczestników o nagrywaniu	Tak	Tak	Tak
Przechowywanie nagrań	W ZOOM lub lokalnie	w Office 365 lub lokalnie (opcja)	w Cisco
Szyfrowanie danych w spoczynku (np. nagrania)	deklaracja ograniczenia dostępu do materiałów użytkownika	Tak (na zasadach określonych dla usług Office 365)	deklaracja ograniczenia dostępu do materiałów użytkownika
Wyciszenie uczestników	Tak	Tak	Tak
Zabezpieczenie pokoju	Klucz 1-16 cyfr	dostęp kontrolowany przez organizatora, możliwość nadania PIN	PIN
Monitorowanie uwagi uczestników	Jako opcja organizatora	? brak informacji	Jako opcja organizatora[35]

Podsumowanie

Z analizy powyższych informacji (bazujących na deklaracjach dostawców usług) wynika, że, zasadniczo, wszyscy dostawcy deklarują stosowanie środków bezpieczeństwa na porównywalnym poziomie. Wyjątkiem jest Microsoft, który nie deklaruje szyfrowania End-2-End. Brak stosowania szyfrowania End-2-End może, ale niekoniecznie oznacza brak poufności. Wszak klient jest związany umową z Microsoft. Zgodnie z deklaracją Microsoft, o każdym dostępie do danych klient jest uprzednio informowany. Niemniej jednak brak zastosowania szyfrowania End-2-End podwyższa ryzyko wynikające z korzystania z Teams i pozostawia konieczność podwyższonego zaufania do dostawcy – Microsoft.

Wszyscy dostawcy zapewniają wiele funkcjonalności umożliwiających dostosowanie charakteru spotkań do uzgodnionych w danej sytuacji wymagań oraz wymagań indywidualnych związanych z zapewnieniem bezpieczeństwa. Zakresem niniejszej analizy nie była jednak ocena szczegółowa skuteczności zastosowanych rozwiązań, architektury i środków bezpieczeństwa, zatem przed wykorzystaniem konkretnego rozwiązania zaleca się przeprowadzenie odrębnej oceny technologicznej w tym zakresie.

Na podstawie powyższych ustaleń można potwierdzić zatem, że korzystanie z usług każdego z podmiotów objętych analizą będzie dopuszczalne zgodnie z RODO, a wskazani dostawcy zapewniają odpowiednie gwarancje stosowania przepisów o ochronie danych. Ostateczny wybór rozwiązania powinien być jednak poprzedzony pogłębioną analizą technologiczną /bezpieczeństwa.

Ponadto, w celu zapewnienia bezpieczeństwa użytkowników i dotyczących ich danych osobowych absolutną koniecznością jest zapewnienie świadomego korzystania z wybranych narzędzi – zarówno przez użytkowników, organizatorów, jak też przez administratorów tych narzędzi po stronie organizacji.

Marcin Wielisiej
Data Processing Architects Sp. o. o.

[35] https://help.webex.com/en-us/st7tr1/Track-Participant-Attention-in-Cisco-Webex-Training#ID_2703_00001140

Źródła i materiały:

ZOOM

- https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf
- https://zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf
- https://zoom.us/terms

TEAMS

- https://www.microsoft.com/en-us/licensing/product-licensing/products
- https://www.microsoft.com/pl-pl/servicesagreement/

CISCO WEBEX

- https://www.cisco.com/c/pl_pl/about/legal/privacy-full.html
- https://www.cisco.com/c/en/us/about/trust-center.html#~resources
- https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf

INNE/CIEKAWE:

- https://www.reuschlaw.de/en/news/berlin-data-protection-authority-position-paper-and-a-checklist-on-the-issue-of-data-protection-in/
- https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Heimarbeit.pdf
- https://www.consumerreports.org/video-conferencing-services/videoconferencing-privacy-issues-google-microsoft-webex/
- https://niebezpiecznik.pl/post/narzedzia-do-rozmow-i-konferencji-wideo-z-szyfrowaniem-end-to-end-krotki-przeglad/
- https://zaufanatrzeciastrona.pl/post/pulapki-wideokonferencji-czyli-czy-zoom-jest-taki-zly/

Warszawa, dnia 18 czerwca 2020 r.

Stanowisko Komisji Etyki i Wykonywania Zawodu Krajowej Rady Radców Prawnych dotyczące zaleceń dla radców prawnych w zakresie stosowania jako formy kontaktu z klientami przy wykonywaniu czynności zawodowych poczty elektronicznej (electronic mail)

Przedmiot sprawy.

W dniu 29 maja 2020r. do Komisji Etyki i Wykonywania Zawodu Krajowej Rady Radców Prawnych skierowana została prośba Prezesa Krajowej Rady Radców Prawnych Macieja Bobrowicza w sprawie wyrażenia stanowiska dotyczącego zaleceń dla radców prawnych w zakresie stosowania jako formy kontaktu z klientami przy wykonywaniu czynności zawodowych poczty elektronicznej (electronic mail). Związane jest to z formułowanymi w związku ze stanem epidemii na obszarze Rzeczypospolitej Polskiej oczekiwaniami co do zalecanych przez organy samorządu zawodowego form komunikowania się z klientami, w szczególności z uwagi na wprowadzoną możliwość wykonywania przez pracowników, w szczególności radców prawnych, pracy zdalnej oraz wprowadzone zalecenia dotyczące ograniczania kontaktów osobistych.

Źródła prawa i materiały wykorzystane do zajęcia stanowiska.

Dla przedstawienia stanowiska w sprawie, oparto się na następujących przepisach prawa:

6) Ustawa z dnia 6 lipca 1982r. o radcach prawnych (Dz.U. z 2020r. poz. 75 z późn. zm.) – art. 3 ust. 3 i ust. 4;
7) Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. z 2020r. poz. 374 z późn. zm.);
8) Rozporządzenie Ministra Zdrowia z dnia 20 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu epidemii (Dz.U. z 2020r. poz. 491 z późn. zm.);
9) Rozporządzenie Rady Ministrów z dnia 29 maja 2020r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii (Dz.U. z 2020r. poz. 964 z późn. zm.);
10) Kodeks Etyki Radcy Prawnego - Uchwała Nr 3/2014 Nadzwyczajnego Krajowego Zjazdu Radców Prawnych z dnia 22 listopada 2014r. w sprawie Kodeksu Etyki Radcy Prawnego – art. 9, art. 15, art. 22, art. 23, art. 35;
11) Regulamin wykonywania zawodu radcy prawnego – Uchwała Nr 94/IX/2015 Krajowej Rady Radców Prawnych z dnia 13 czerwca 2015r. w sprawie Regulaminu wykonywania zawodu radcy prawnego – §6, §10 ust. 1 w związku z §2 pkt 8);

oraz wykorzystano następujące materiały:

3) Włodzimierz Chróścik, Gerard Dźwigała, Leszek Korczak, Tomasz Scheffler, Jarosław Sobutka, Anita Woroniecka, Kodeks Etyki Radcy Prawnego. Komentarz, 2. Wydanie, Wydawnictwo C.H. Beck, Warszawa 2017;
4) Tomasz Jaroszyński, Anna Sękowska, Paweł Skuczyński, Kodeks Etyki Radcy Prawnego. Komentarz, Wydawnictwo Praktyka Prawnicza, Warszawa 2016.

Analiza zagadnienia.

3.1. Poczta elektroniczna jest od wielu lat powszechnie używanym narzędziem technicznym do kontaktów radców prawnych z klientami w związku ze świadczeniem pomocy prawnej. Obowiązujący na obszarze Rzeczypospolitej Polskiej stan epidemii przyczynia się do zwiększenia częstotliwości wykorzystania tej formy kontaktu. Nie zmienia jednak jej istoty, która polega na przesyłaniu w czasie rzeczywistym korespondencji umożliwiającej kontakt między osobami korzystającymi z tego narzędzia.

3.2. Przepisy prawa powszechnie obowiązującego, w szczególności ustawa z dnia 6 lipca 1982r. o radcach prawnych, ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, rozporządzenie Ministra Zdrowia z dnia 20 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu epidemii oraz rozporządzenie Rady Ministrów z dnia 29 maja 2020r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii nie zawierają szczególnych regulacji dotyczących zasad korzystania z narzędzia technicznego w formie poczty elektronicznej w wykonywaniu zawodu radcy prawnego.

Z uwagi na okoliczność, że poczta elektroniczna jest narzędziem technicznym powszechnie używanym przy wykonywaniu zawodu radcy prawnego uwzględnienia wymagają przy korzystaniu m.in. z tego środka komunikacji przepisy ogólne ustawy z dnia 6 lipa 1982r. o radcach prawnych, tj. art. 3 ust. 3 i 4 zgodnie z którymi radca prawny jest obowiązany zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzieleniem pomocy prawnej, przy czym obowiązek ten nie może być ograniczony w czasie. Zachowanie tajemnicy zawodowej oznacza bowiem w szczególności zabezpieczenie przekazywanych przy wykorzystaniu poczty elektronicznej informacji przed ujawnieniem w szczególności osobom nieuprawionym (niepowołanym), z zastrzeżeniem, że pod pojęciem ujawnienia rozumieć należy dostęp do poczty elektronicznej, utrwalenie lub odtworzenie wiadomości przekazywanych przy jej pomocy w całości lub w części w celu wykorzystania przekazanych informacji w każdej postaci, zarówno nieprzetworzonej, jak i przetworzonej.

3.3. Uwagi wymagają również przepisy prawa wewnętrznego.

A. W pierwszej kolejności zwrócić należy uwagę na zasadę ogólną wyrażoną w art. 9 Kodeksu Etyki Radcy Prawnego zgodnie z którą dochowanie tajemnicy zawodowej jest prawem i obowiązkiem radcy prawnego, stanowi przy tym podstawę zaufania klienta i jest gwarancją praw i wolności. Zasada ta została rozwinięta w przepisach Działu III Kodeksu w Rozdziale 1. dotyczącym tajemnicy zawodowej. Wskazać tutaj należy na przepis art. 15, który w ocenie Komisji Etyki i Wykonywania Zawodu Krajowej Rady Radców Prawnych powinien znaleźć odpowiednie zastosowanie w przypadku poczty elektronicznej jako środka kontaktu radcy prawnego z klientem, ale przede wszystkim art. 23, który stanowi, co następuje:

Art. 23
Radca prawny obowiązany jest zabezpieczyć przed niepowołanym ujawnieniem wszelkie informacje objęte tajemnicą zawodową, niezależnie od ich formy i sposobu utrwalenia. Dokumenty i nośniki zawierające informacje poufne należy przechowywać w sposób chroniący je przed zniszczeniem, zniekształceniem lub zaginięciem. Dokumenty i nośniki przechowywane

w formie elektronicznej powinny być objęte odpowiednią kontrolą dostępu oraz zabezpieczeniem systemu przed zakłóceniem działania, uzyskaniem nieuprawnionego dostępu lub utratą danych. Radca prawny powinien kontrolować dostęp osób współpracujących do takich dokumentów i nośników.

Zwrócić bowiem należy uwagę, że za jedną z form utrwalania informacji uznać należy pocztę elektroniczną z uwagi na okoliczność, iż za jej pomocą dokonywana jest rejestracja przekazywanych przy jej pomocy wiadomości, co pozwala na dostęp zarówno do treści samej wiadomości, jak również do prezentowanych, czy załączonych dokumentów, które mogą być widoczne i możliwe dla odczytania przez osoby korzystające z tego narzędzia w istocie w dowolnym czasie. W przypadku utrwalenia wiadomości, w tym dokumentów, na nośniku informacji zastosowanie powinny także znaleźć cytowane wyżej postanowienia dotyczące nośników.

Przypomnieć w tym miejscu także trzeba, że radca prawny powinien wyraźnie zobowiązać osoby współpracujące z nim przy wykonywaniu czynności zawodowych do zachowania poufności w zakresie objętym jego tajemnicą zawodową, wskazując na ich odpowiedzialność prawną związaną z ujawnieniem tajemnicy zawodowej (art. 22 Kodeksu etyki Radcy Prawnego) oraz podjąć wszelkie niezbędne czynności w celu zapewnienia przestrzegania zakazu ujawniania informacji objętych tajemnicą zawodową radcy prawnego przez osoby niezwiązane tajemnicą zawodową na mocy ustawy, z pomocą których radca prawny wykonuje czynności związane ze świadczeniem pomocy prawnej (§6 ust. 1 Regulaminu wykonywania zawodu radcy prawnego). W przypadku tej ostatniej kategorii osób radca prawny przed dopuszczeniem ich do wykonywania czynności związanych ze świadczeniem pomocy prawnej ma obowiązek wymagać złożenia pisemnego oświadczenia zawierającego zobowiązanie do przestrzegania obowiązku zachowania w tajemnicy wszelkich informacji, o których dowiedziały się w związku z wykonywaniem tych czynności, przy czym oświadczenie może być złożone na wzorze stanowiącym załącznik do Regulaminu wykonywania zawodu radcy prawnego (§6 ust. 1 Regulaminu wykonywania zawodu radcy prawnego).

Szczególnej uwagi wymaga także przepis art. 35 Kodeksu Etyki Radcy Prawnego, zamieszczony wprawdzie w rozdziale dotyczącym informowania o wykonywaniu zawodu oraz pozyskiwania klientów, ale odnoszący się wprost także do wykonywania czynności zawodowych drogą elektroniczną. W ocenie Komisji Etyki i Wykonywania Zawodu znajduje on zastosowanie w przypadku stosowania, jako formy kontaktu z klientami, poczty elektronicznej.

W literaturze przedmiotu zgodnie bowiem przyjmuje się, że Kodeks Etyki Radcy Prawnego nie definiuje pojęcia „*droga elektroniczna*" i w konsekwencji „(…) *można uznać za uzasadnione posiłkowe posługiwanie się definicją „świadczenie usługi drogą elektroniczną"*

z ustawy z 18.7.2002r. o świadczeniu usług drogą elektroniczną (…).” (cyt. za: Gerard Dźwigała [w:] Włodzimierz Chróścik, Gerard Dźwigała, Leszek Korczak, Tomasz Scheffler, Jarosław Sobutka, Anita Woroniecka, Kodeks Etyki Radcy Prawnego. Komentarz, 2. Wydanie, Wydawnictwo C.H. Beck, Warszawa 2017 – komentarz do art. 35 teza 10, s. 220; zob. także: Anna Sękowska [w:] Tomasz Jaroszyński, Anna Sękowska, Paweł Skuczyński, Kodeks Etyki Radcy Prawnego. Komentarz, Wydawnictwo Praktyka Prawnicza, Warszawa 2016 – komentarz do art. 35, teza 1., s. 172). Zgodnie z art. 2 pkt 4) ustawy z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną pod pojęciem świadczenia usług drogą elektroniczną rozumieć należy wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne. Z uwagi na wskazane cechy przyjąć należy, że wykonywanie czynności zawodowych z wykorzystaniem tego środka komunikacji na odległość jest świadczeniem usług drogą elektroniczną, a zatem znajduje w tym przypadku zastosowanie art. 35 Kodeksu Etyki Radcy Prawnego.

Dla porządku przytoczyć wypada jego treść:

Art. 35.
Radca prawny może informować o wykonywaniu zawodu, pozyskiwać klientów oraz wykonywać czynności zawodowe drogą elektroniczną, jeśli:
1) jest zawsze jednoznacznie identyfikowalny jako nadawca lub odbiorca, w szczególności poprzez adresy poczty elektronicznej lub inne identyfikatory;
2) nie korzysta z drogi elektronicznej w sposób anonimowy lub na rzecz osób, których nie można jednoznacznie zidentyfikować jako konkretnych klientów lub odbiorców czy nadawców w komunikacji, w szczególności w Internecie;
3) nie korzysta z form aktywności dostępnych drogą elektroniczną w sposób sprzeczny z prawem, dobrymi obyczajami i zasadami Kodeksu, w szczególności tworząc rozwiązania skutkujące nieprawdziwymi, wprowadzającymi w błąd, ocennymi oznaczeniami lub informacjami, lub w sposób utrudniający innym radcom prawnym dostęp do rynku;
4) korzysta z form aktywności dostępnych drogą elektroniczną w sposób gwarantujący oddzielenie wykonywania zawodu od swoich prywatnych przekonań, poglądów, postaw i działań oraz innej działalności zawodowej;
5) nie wydaje, nie inspiruje lub nie płaci osobom trzecim za wydawanie pozytywnych lub negatywnych opinii, komentarzy, poleceń, rekomendacji bądź referencji dotyczących wykonywania zawodu przez siebie lub inne osoby, z którymi może na podstawie przepisów prawa wspólnie wykonywać zawód, w szczególności w sposób anonimowy, nieprawdziwy lub wprowadzający w błąd;
6) poprzez okresową archiwizację zabezpiecza i dba o dostępność danych przetwarzanych drogą elektroniczną;
7) chroni tajemnicę zawodową, informując w treści korespondencji elektronicznej o jej poufnym charakterze; zabezpieczenie uznaje się za należyte, jeżeli klient po uprzednim poinformowaniu go o zagrożeniach związanych z korzystaniem z drogi elektronicznej, domyślnie lub wyraźnie zaakceptował

stosowane w komunikacji z nim środki, techniki, sposoby, systemy lub standardy komunikacji elektronicznej.

Zwrócić należy uwagę, że cytowany przepis dotyczy nie tylko wymagań dotyczących wykonywania przez radcę prawnego czynności zawodowych drogą elektroniczną, ale także informowania o wykonywaniu zawodu oraz pozyskiwania klientów. Komisja Etyki i Wykonywania Zawodu Krajowej Rady Radców Prawnych podziela przy tym pogląd Gerarda Dźwigały, że wykonywania czynności zawodowych dotyczą pkt 1), 2), 4) oraz 6) i 7) (zob.: Gerard Dźwigała, op. cit. – komentarz do art. 35 teza 8, s. 220).

B. Przechodząc z kolei do Regulaminu wykonywania zawodu radcy prawnego wskazać należy, że w przypadku utrwalenia wiadomości, w tym dokumentów, przekazywanych za pomocą poczty elektronicznej na nośniku zapewnić trzeba należyte warunki jego przechowywania, zabezpieczając przed zniszczeniem, zaginięciem i przed dostępem osób niepowołanych, a to zgodnie z postanowieniami §10 ust. 1 w związku z §2 pkt 8).

Podsumowanie

Wskazując na ogólną zasadę dotyczącą obowiązku przestrzegania tajemnicy zawodowej, rozumianego w szczególności jako obowiązek zachowania, zapewnienia i zabezpieczenia tej tajemnicy, Komisja Etyki i Wykonywania Zawodu Krajowej Rady Radców Prawnych dla jego potrzeb w przypadku korzystania z poczty elektronicznej, jako formy kontaktu z klientami przy wykonywaniu czynności zawodowych podnosi, co następuje:

A. Obowiązek przestrzegania tajemnicy zawodowej oznacza konieczność zapewnienia środków technicznych i organizacyjnych mających zabezpieczyć przed jej ujawnieniem, w szczególności dostępem do poczty elektronicznej osób nieuprawnionych (niepowołanych). Zalecić należy okresowe przeglądy zasobów poczty elektronicznej radcy prawnego oraz trwałe usuwanie wiadomości, w tym załączników, których archiwizacja w skrzynce pocztowej nie jest niezbędna albo istnieje obowiązek ich usunięcia.

B. W przypadku korzystania przez radcę prawnego z poczty elektronicznej zalecić należy dołożenie przez radcę prawnego staranności wymaganej od profesjonalisty w zakresie zapewnienia narzędzia posiadającego zabezpieczenia chroniące przed dostępem osób nieuprawnionych do poczty elektronicznej, ujawnieniem wiadomości, w tym dokumentów, przekazywanych przy jej wykorzystaniu, czy możliwości odtworzenia tych wiadomości, w tym

dokumentów, przy czym w przypadku braku wystarczającej wiedzy w tym zakresie – skorzystanie z pomocy osoby dysponującej specjalistyczną wiedzą w tym zakresie.

C. W przypadku korzystania z poczty elektronicznej przez klienta radca prawny powinien uprzedzić go o możliwych ryzykach związanych z używaniem tego narzędzia oraz o konieczności wyboru odpowiednich zabezpieczeń.

D. W przypadku utrwalenia wiadomości, w tym dokumentów, przekazywanych z wykorzystaniem poczty elektronicznej na nośniku informacji należy postępować z nim zgodnie z zasadami określonymi w Kodeksie Etyki Radcy Prawnego oraz Regulaminie wykonywania zawodu radcy prawnego.

E. Ponadto Komisja Etyki i Wykonywania Zawodu Krajowej Rady Radców Prawnych uznaje za zasadne systematyczne zapoznawanie się radców prawnych z zaleceniami i rekomendacjami właściwych administratorów poczty elektronicznej dotyczącymi zasad korzystania z tego narzędzia, w tym zasad bezpieczeństwa, oraz rozważenie stosowania się do nich.

Opracowanie:
r.pr. Grzegorz Wyszogrodzki

Przewodniczący
Komisji Etyki i Wykonywania Zawodu
Krajowej Rady Radców Prawnych
r.pr. Ryszard Wilmanowicz

Rekomendacje dla radców prawnych: Bezpieczeństwo poczty elektronicznej w praktyce wykonywania zawodu radcy prawnego w kontekście obowiązku zachowania tajemnicy zawodowej oraz ochrony danych osobowych

Warszawa, dnia 30 kwietnia 2020 r.

1. Przedmiot rekomendacji

1.1. Celem niniejszego dokumentu jest przedstawienie rekomendacji w zakresie przesyłania informacji objętych tajemnicą zawodową lub danych osobowych przez radców prawnych za pośrednictwem poczty elektronicznej.

1.2. Ponadto, niniejszy dokument wyjaśnia:

(1) dlaczego radca prawny musi chronić komunikację z użyciem poczty elektronicznej;

(2) jakie zagrożenia mogą wynikać z korzystania przez radców prawnych z poczty elektronicznej;

(3) jakie środki zabezpieczające może stosować radca prawny w związku z korzystaniem z poczty elektronicznej, aby przeciwdziałać tym zagrożeniom.

1.3. Co do zasady, można zidentyfikować dwa główne obszary zagrożeń związanych z korzystaniem przez radcę prawnego z poczty elektronicznej:

(1) po pierwsze, są to **zagrożenia związane z przesyłaniem i odbieraniem informacji prawnie chronionych przez radcę prawnego przy użyciu poczty elektronicznej**, oraz

(2) po drugie, są to **zagrożenia dla całego systemu teleinformatycznego wynikające z korzystania przez radcę prawnego z poczty elektronicznej.**

Tym dwóm obszarom zagrożeń przyporządkowane zostały szczegółowe rekomendacje co do tego, jak radca prawny może przeciwdziałać tego typu zagrożeniom.

2. Dlaczego radca prawny musi zapewnić bezpieczeństwo poczty elektronicznej?

2.1. Radca prawny korzystając z poczty elektronicznej powinien pamiętać o spoczywających na nim obowiązkach w zakresie ochrony informacji związanych z wykonywaniem zawodu. Wspomniane obowiązki zobowiązują radcę prawnego do zachowania **poufności** informacji, ale także jej **integralności** i **dostępności.**

2.2. Obowiązki radcy prawnego w tym zakresie wynikają w szczególności z przepisów prawa dotyczących:

(1) **ochrony tajemnicy zawodowej** (tajemnicy radcy prawnego), oraz

(2) **ochrony danych osobowych**.

2.3. Obowiązek zachowania tajemnicy przez radcę prawnego nie ogranicza się do zakazu ujawniania tajnych informacji, ale rozciąga się na **potrzebę zabezpieczenia procesu komunikacji z klientem i innymi osobami, tak aby nieuprawnione osoby trzecie nie miały dostępu do tych informacji.** Powyższy obowiązek dotyczy każdego sposobu komunikacji – i tradycyjnej, i elektronicznej. Za naruszenie tajemnicy może zostać uznane już takie zaniechanie, poprzez brak zabezpieczeń komunikacji lub ich

niewystarczający poziom, które tylko stworzy możliwość dostępu do poufnych informacji nieuprawnionym podmiotom.

2.4. Jeżeli przedmiotem przetwarzanych przez radcę prawnego informacji są **dane osobowe** to niezależnie od obowiązku zachowania tajemnicy zawodowej, do przesyłania przez niego danych osobowych znajdą zastosowanie przepisy o ochronie danych osobowych, w tym przede wszystkim RODO.

2.5. RODO wymaga, aby dane osobowe były przetwarzane w sposób zapewniający **odpowiednie bezpieczeństwo** tych danych, w tym **ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych** („integralność i poufność") (art. 5 ust. 1 lit. f) RODO). Wspomniane środki powinny zostać również przedsięwzięte w procesach przekazywania (komunikacji) danych osobowych.

2.6. Radca prawny korzystając z poczty elektronicznej powinien być świadomy zagrożeń w obu wyżej wspomnianych obszarach, tj. (1) związanych z przesyłaniem i odbieraniem informacji prawnie chronionych przez radcę prawnego przy użyciu poczty elektronicznej, oraz (2) wynikających z korzystania przez radcę prawnego z poczty elektronicznej dla całego systemu teleinformatycznego, z którego korzysta.

2.7. Przypomnijmy, że radca prawny jest zobowiązany do zachowania **poufności**, **integralności** i **dostępności** informacji:

- **Poufność** oznacza właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
- **Integralność** oznacza właściwość zapewnienia dokładności i kompletności aktywów (zasobów).
- **Dostępność** oznacza właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.

2.8. Zagrożenia dotyczące powyższych atrybutów bezpieczeństwa informacji w odniesieniu do korzystania z poczty elektronicznej można przedstawić następująco:

- Zagrożenie dotyczące **poufności** informacji przesyłanych pocztą elektroniczną może polegać na tym, że osoba nieuprawniona zapozna się z treścią wiadomości e-mail przesyłanej radcę prawnego lub do niego.
- Zagrożenie dotyczące **integralności** informacji przesyłanych pocztą elektroniczną może polegać na tym, że osoba nieuprawniona „przechwyci" wiadomość przesyłaną przez radcę prawnego lub do niego i zmieni treść tej wiadomości.
- Zagrożenie dotyczące **dostępności** informacji przesyłanych pocztą elektroniczną może polegać na tym, że osoba nieuprawniona „przechwyci" wiadomość i w ogóle nie dojdzie ona do adresata, albo dojdzie z opóźnieniem.

3. Rekomendacje dotyczące przesyłania i odbierania informacji prawnie chronionych przy użyciu poczty elektronicznej

3.1. Rekomendacje dzielą się na:

1) rekomendacje dotyczące sposobów ochrony przesyłanych informacji;
2) rekomendacje dotyczące przesyłania informacji objętych tajemnicą zawodową lub danych osobowych za pośrednictwem poczty elektronicznej, w tym komunikacji z klientem;
3) rekomendacje dotyczące wyboru dostawcy.

Rekomendacje dotyczące sposobów ochrony przesyłanych informacji

Co powinien sprawdzić radca prawny przesyłając informacje prawnie chronione przy użyciu poczty elektronicznej?

3.2. Radca prawny powinien sprawdzić i być świadomy tego, w jaki sposób zabezpieczane są wiadomości e-mail, które są wysyłane z jego skrzynki poczty elektronicznej.

3.3. 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 informacji poufne bez żadnych zabezpieczeń**.

3.4. Poniżej przedstawione są trzy najczęściej stosowane sposoby zabezpieczenia informacji przesyłanych przy użyciu poczty elektronicznej:

(1) **Szyfrowanie podczas przesyłania przy użyciu protokołu TLS** (ang. *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.

(2) **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).

(3) **Szyfrowanie załączników do wiadomości e-mail**

Jest to sposób zabezpieczenia niezależny od powyższych rozwiązań i polega na zaszyfrowaniu załącznika do wiadomości e-mail i przesłanie go w takiej formie do odbiorcy. Hasło (klucz) do zaszyfrowanego pliku powinien być przekazany odbiorcy innym bezpiecznym kanałem (np. telefonicznie, przez SMS).

Rekomendacje dotyczące przesyłania informacji objętych tajemnicą zawodową lub danych osobowych za pośrednictwem poczty elektronicznej, w tym komunikacja z klientem

Jakie działania powinien podjąć radca prawny, by lepiej chronić informacje przesyłane za pośrednictwem poczty elektronicznej?

3.5. 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 radcą prawnym za pomocą tego kanału komunikacji.

3.6. Rekomendowane byłoby 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 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).

3.7. 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.

3.8. Jednocześnie w takiej informacji dla klienta należałoby zaznaczyć, że jeżeli klient będzie korzystał z poczty elektronicznej do przekazywania radcy prawnemu informacji poufnych bez ustalania ewentualnych dodatkowych zabezpieczeń, to klient wyraża zgodę na stosowanie takiej formy komunikacji mimo potencjalnych związanych z tym ryzyk.

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

3.10. Radca prawny powinien stosować odpowiednie zabezpieczenia informacji przekazywanych pocztą elektroniczną także w przypadku **przekazywania przez radcę prawnego 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).

3.11. 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. Odradza się zbędne wysyłanie pocztą elektroniczną korespondencji, która została lub ma być przekazana do organu w inny sposób (np. przez ePUAP, pocztą tradycyjną, osobiście).

3.12. Ponadto, **do każdej wiadomości e-mail radca prawny powinien załączać krótką informację, 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 (radcę prawnego) i trwale tę wiadomość usunąć.

3.13. 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).

Rekomendacje dotyczące wyboru dostawcy

Jakie warunki powinien spełnić radca prawny przy zawieraniu umowy z dostawcą poczty elektronicznej?

3.14. Radca prawny wybierając dostawcę poczty elektronicznej powinien kierować się **koniecznością zachowania tajemnicy zawodowej** zgodnie z ustawą o radcach prawnych, Kodeksem Etyki Radcy Prawnego i Regulaminem wykonywania zawodu radcy prawnego, oraz **przepisami o ochronie danych osobowych**.

3.15. W związku z korzystaniem z poczty elektronicznej informacje prawnie chronione (w tym dane osobowe) będą przekazywane (powierzane) do zewnętrznego dostawcy.

3.16. W tym przypadku kancelaria radcy prawnego lub spółka[36], w której wykonuje on zawód będzie **administratorem danych**, a dostawca usługi poczty elektronicznej - **podmiotem przetwarzającym** w rozumieniu RODO, gdyż przetwarza on w imieniu administratora dane osobowe znajdujące się w wiadomościach.

3.17. Przepisy o ochronie danych osobowych dopuszczają korzystanie przez administratora z zewnętrznego podmiotu przetwarzającego (tu: dostawcy poczty elektronicznej), ale jednocześnie ustanawiają **warunki, jakie powinien spełnić administrator powierzając przetwarzanie danych osobowych.**

3.18. **Administrator** (kancelaria radcy prawnego lub spółka, w której wykonuje on zawód) musi:

(1) **wybrać dostawcę poczty elektronicznej, który spełnia wymogi RODO**, oraz
(2) **zawrzeć z nim umowę powierzenia** o określonej treści (art. 28 ust. 3 RODO).

[36] Chodzi o sytuację, w której radca prawny wykonuje zawód w spółce, której wyłącznym przedmiotem działalności jest świadczenie pomocy prawnej, w formach określonych w art. 8 ust. 1 URP. W takiej sytuacji administratorem danych osobowych jest właśnie spółka.

3.19. Administrator powinien korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą (art. 28 ust. 1 RODO). Obowiązek ten został wyjaśniony bardziej szczegółowo w motywie 81 do RODO, w którym wskazano, że administrator powinien korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje co do **wiedzy fachowej, wiarygodności i zasobów**. Administrator powinien sprawdzić powyższe gwarancje przed powierzeniem podmiotowi przetwarzającemu czynności przetwarzania.

Jako **wiedzę fachową** należy rozumieć doświadczenie dostawcy w świadczeniu usług związanych z przetwarzaniem danych, powołanie inspektora ochrony danych lub – gdy nie jest to wymagane – koordynatora ds. ochrony danych czy też przeszkolenie pracowników z zakresu ochrony danych i bezpieczeństwa informacji. O **wiarygodności** dostawcy będzie w przyszłości świadczyć stosowanie zatwierdzonego kodeksu postępowania (art. 40 RODO) lub zatwierdzonego mechanizmu certyfikacji (art. 42 RODO). Jako **zasoby** należy natomiast rozumieć wdrożenie polityk i procedur związanych z ochroną danych, wdrożenie zasad bezpieczeństwa informacji zgodnie z normami ISO 27000, wdrożenie środków technicznych i organizacyjnych, takich jak szyfrowanie podczas przesyłania lub szyfrowanie treści wiadomości e-mail.

3.20. Należy pamiętać, że to na kancelarii radcy prawnego lub spółce, w której wykonuje on zawód jako administratorze danych ciąży obowiązek wykazania, że przed wyborem dostawcy dokonano analizy pod kątem zapewniania przez niego gwarancji, o których mowa w RODO (art. 28 ust. 1 RODO).

3.21. Jeżeli radca prawny nie posiada wiedzy pozwalającej na ocenę bezpieczeństwa poszczególnych narzędzi, to powinien on skorzystać z pomocy innego radcy prawnego, eksperta w zakresie bezpieczeństwa informacji lub też pogłębić wiedzę w tym zakresie samodzielnie.

3.22. Administrator jest jednocześnie zobowiązany do **zawarcia umowy powierzenia przetwarzania danych**, która powinna określać zasady wykonywania przez dostawcę obowiązków, o których mowa w art. 28 ust. 3 RODO. Umowa powierzenia powinna w szczególności zobowiązywać podmiot przetwarzający do:

- zachowania tajemnicy, w tym zapewniania, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy (art. 28 ust. 3 lit. b) RODO);
- podejmowania wszelkich środków wymaganych na mocy art. 32 RODO, czyli w zakresie bezpieczeństwa danych osobowych (art. 28 ust. 3 lit. c) RODO), w szczególności zapewnienia odpowiednich zabezpieczeń poczty elektronicznej;
- pomagania administratorowi wywiązać się z obowiązków określonych w art. 32-36 RODO, czyli w zakresie zapewnienia bezpieczeństwa danych osobowych, zarządzania naruszeniami ochrony danych oraz przeprowadzania oceny skutków dla ochrony danych (art. 28 ust. 3 lit. f) RODO);

- udostępniania administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwienia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynianie się do nich (art. 28 ust. 3 lit. h) RODO);
- zgłaszania administratorowi naruszeń ochrony danych osobowych niezwłocznie po ich stwierdzeniu (art. 33 ust. 2 RODO).

3.23. W tym kontekście **zalecane jest ostrożne korzystanie z „darmowych" skrzynek poczty elektronicznej**, w tym dokładne sprawdzenie warunków świadczenia usług pod kątem zgodności z przepisami prawa i zasadami bezpieczeństwa informacji.

3.24. Trzeba zwrócić szczególną uwagę na te warunki świadczenia usług, których stosowanie w odniesieniu do radcy prawnego mogłoby spowodować, że nie spełniałby on ciążących na nim obowiązków dotyczących ochrony tajemnicy zawodowej lub ochrony danych osobowych. Do takich warunków należą w szczególności:

- postanowienie, że dostawca usług poczty elektronicznej będzie wykorzystywać informacje znajdujące się w skrzynce poczty elektronicznej do własnych celów (np. statystycznych) – w takiej sytuacji może dojść do **naruszenia poufności informacji** znajdujących się w skrzynce (co byłoby również naruszeniem art. 5 ust. 1 lit. f) RODO);
- postanowienie, że po określonym czasie nielogowania do poczty elektronicznej przez użytkownika, zawartość skrzynki elektronicznej zostanie usunięta – w takiej sytuacji może dojść do **naruszenia dostępności informacji** znajdujących się w skrzynce (co byłoby również naruszeniem art. 32 ust. 1 RODO);
- warunki świadczenia usług, które nie spełniają wymogów dotyczących umowy powierzenia przetwarzania określonych w art. 28 ust. 3 RODO (co byłoby również naruszeniem tego przepisu RODO).

3.25. Przy wyborze dostawcy poczty elektronicznej należy również zwrócić uwagę, czy dane osobowe będą przetwarzane na terenie Europejskiego Obszaru Gospodarczego, czy też poza nim, ze względu na ograniczenia dotyczące transferu danych poza EOG wynikające z RODO. **Jeżeli zgodnie z umową dostawca poczty elektronicznej mógłby przechowywać zawartość skrzynki pocztowej radcy prawnego poza EOG, to należy sprawdzić, czy w danym państwie zapewniony jest odpowiedni poziom ochrony lub zapewniono odpowiednie zabezpieczenia w rozumieniu art. 45-47 RODO.**

3.26. Szczegółowe informacje dotyczące przekazywania danych osobowych do państw trzecich (poza EOG) znajdują się na stronie Urzędu Ochrony Danych Osobowych (UODO)[37] oraz na stronie Komisji Europejskiej[38].

[37] UODO, „RODO ma zapewnić ochronę także w państwach trzecich, do których są przekazywane dane", dostępne pod adresem: https://uodo.gov.pl/pl/189/737. Prezentacja ze szkolenia prowadzonego przez UODO na temat przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych znajduje się pod adresem: https://uodo.gov.pl/pl/file/1973.

[38] Komisja Europejska, „Jakie przepisy stosuje się w przypadku organizacji przekazującej dane do krajów spoza UE?", dostępne pod adresem: https://ec.europa.eu/info/law/law-topic/data-

4. Zagrożenia i rekomendacje dotyczące korzystania przez radcę prawnego z poczty elektronicznej dla całego systemu teleinformatycznego

Najczęstsze zagrożenia dla bezpieczeństwa informacji w związku z korzystaniem z poczty elektronicznej dla systemu teleinformatycznego

4.1. Niezależnie od powyżej przedstawionych zagrożeń dotyczących poufności przesyłanej korespondencji, poczta elektroniczna może być **źródłem zagrożenia dla całego systemu informatycznego, z którego korzysta radca prawny** oraz informacji w nim zawartych.

4.2. Przy obecnym rozwoju technologii dynamicznie zmieniają się zagrożenia w związku z korzystaniem z internetu i poczty elektronicznej. Obecnie najczęściej występujące zagrożenia mogące mieć znaczenie dla korzystania z poczty elektronicznej to:

- ***phishing***
- ***malware oraz***
- ***ransomware***.

4.3. Zagrożenia te są opisane poniżej. Należy jednak pamiętać, że **istnieją także inne rodzaje zagrożeń związane zarówno z korzystaniem z poczty elektronicznej, jak i dotyczące ogólnie pojmowanego bezpieczeństwa informacji.**

Phishing jest to metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań.

4.4. **Phishing** może polegać w szczególności na:

- wysyłaniu wiadomości przez podszywających się pod dostawców w celu wyłudzeniu płatności,
- wyłudzaniu poświadczeń do kont (hasło, login),
- wysyłaniu fałszywych faktur na adres e-mail przez podmioty podszywające się np. pod dostawców telekomunikacyjnych,
- wysyłaniu informacji o nieautoryzowanym logowaniu w celu nakłonienia do podania danych do logowania na fałszywej stronie internetowej.

protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_pl.

Malware to ogół programów mających szkodliwe działanie w stosunku do systemu komputerowego lub jego użytkownika (zbitka słów *malicious* „złowrogi, złośliwy” i *software* „oprogramowanie”).

4.5. W związku z korzystaniem z poczty elektronicznej **należy zwracać uwagę na załączniki i linki w wiadomościach od nieznanych lub niebudzących zaufania nadawców**, których otworzenie może zainicjować zainstalowanie złośliwego oprogramowania, które może spowodować zarówno utratę poufności danych, jak i ich integralności.

Ransomware to typ szkodliwego oprogramowania, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych (często poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego (zbitka słów *ransom* „okup” i *software* „oprogramowanie”).

Rekomendacje dotyczące korzystania przez radcę prawnego z poczty elektronicznej w celu ochrony systemu teleinformatycznego

4.6. **Należy każdorazowo weryfikować adres e-mail nadawcy**, w tym sprawdzić, czy nadawca jest znany lub czy adres e-mail nadawcy zgadza się z dotychczas stosowanym adresem.

4.7. Jeżeli radca prawny zna osobę nadawcy (np. Jan Kowalski), powinien on sprawdzić, czy dany adres e-mail odpowiada adresowi e-mail, z którego otrzymywał on poprzednie wiadomości od tego nadawcy. Często fałszywe adresy e-mail mogą różnić się w niewielkim zakresie od prawdziwych adresów e-mail (np. @oirpwarszawa.com zamiast @oirpwarszawa.pl).

4.8. **Należy zwracać uwagę na treść wiadomości**, zwłaszcza jeżeli otrzymana wiadomość pochodzi od nieznanego nadawcy.

4.9. **Należy zachować szczególną ostrożność klikając w linki lub otwierając załączniki zamieszczone w wiadomości.**

4.10. **Należy zachować w poufności hasła do poczty elektronicznej i regularnie je zmieniać** (np. raz na 3 miesiące). W celu zapewnienia odpowiedniego bezpieczeństwa, hasło nie powinno być oczywiste i łatwe do odgadnięcia przez osoby trzecie. Hasło do służbowej poczty elektronicznej powinno być inne niż hasło do innych skrzynek poczty elektronicznej, sklepów internetowych czy portali społecznościowych. W tym zakresie rozwiązaniem, które można rozważyć, jest korzystanie z tzw. menadżera haseł – narzędzia, które służy do generowania, bezpiecznego przechowywania i automatycznego wprowadzania haseł do poczty elektronicznej oraz innych stron internetowych. Ponadto, jeżeli dostawca poczty elektronicznej zapewnia taką możliwość, zalecane jest korzystanie z uwierzytelniania dwuskładnikowego (weryfikacji dwuetapowej), która polega na wykorzystaniu w trakcie logowania dodatkowego etapu weryfikacji użytkownika (np. wpisanie jednorazowego kodu wysłanego przez usługodawcę za pomocą wiadomości SMS oprócz logowania za pomocą hasła użytkownika).

4.11. **Nie należy wykorzystywać służbowej skrzynki poczty elektronicznej do wysyłania i odbierania wiadomości prywatnych**.

4.12. Służbowy adres e-mail nie powinien być wykorzystywany jako login do portali internetowych wykorzystywanych w celach prywatnych, w tym w szczególności portali społecznościowych.

4.13. **Nie należy przesyłać wiadomości służbowych na prywatne konto poczty elektronicznej.**

4.14. **Należy pamiętać o bieżących aktualizacjach systemu operacyjnego oraz oprogramowania antywirusowego**, które powinno również służyć do ochrony poczty elektronicznej.

4.15. Pozostali pracownicy kancelarii również powinni stosować się do powyższych zasad bezpieczeństwa poczty elektronicznej. W tym celu **należy przeszkolić pracowników kancelarii w zakresie ochrony danych osobowych i podstawowych zasad bezpieczeństwa informacji** oraz zobowiązać ich do stosowania się do powyższych zasad bezpieczeństwa. Szkolenia z zakresu ochrony danych osobowych i bezpieczeństwa informacji powinny być przeprowadzane okresowo. Należy pamiętać, że w przypadku wymienionych zagrożeń to człowiek jest często „najsłabszym ogniwem".

4.16. Poza przedstawionymi środkami należy także stosować środki w celu przeciwdziałania innym zagrożeniom bezpieczeństwa informatycznego, chociażby związane z **bezpieczeństwem fizycznym sprzętu informatycznego lub bezpieczeństwem sieci.**

4.17. Zalecane jest również wprowadzenie w kancelarii **polityki korzystania z poczty elektronicznej**, która powinna uwzględniać powyższe kwestie, lub zamieszczenie tych zasad w polityce bezpieczeństwa informacji. Oprócz tego zwracamy uwagę, że elementem całościowej polityki bezpieczeństwa informacji (polityki ochrony danych) w kancelarii powinny być zasady reagowania na incydenty bezpieczeństwa informacji i naruszenia ochrony danych osobowych. Ze względu na zmiany w technologiach zalecane jest również regularne aktualizowanie tego typu dokumentów.

Uzasadnienie prawne powyższych rekomendacji znajduje się w opinii prawnej dotyczącej bezpieczeństwa poczty elektronicznej w praktyce wykonywania zawodu radcy prawnego w kontekście obowiązku zachowania tajemnicy zawodowej oraz ochrony danych osobowych.

Rekomendacje sporządzone zostały przez zespół Kancelarii Traple, Konarski, Podrecki i Wspólnicy na zlecenie Ośrodka Badań, Studiów i Legislacji Krajowej Rady Radców Prawnych.

Opracowali:

dr Grzegorz Sibiga

dr Iga Małobęcka-Szwast

Dominika Nowak

Katarzyna Syska

Opinia prawna

dotycząca bezpieczeństwa poczty elektronicznej w praktyce wykonywania zawodu radcy prawnego w kontekście obowiązku zachowania tajemnicy zawodowej oraz ochrony danych osobowych

przygotowana na zlecenie:
Krajowej Izby Radców Prawnych z siedzibą w Warszawie, dalej jako: „**KIRP**”

Warszawa, dnia 17 kwietnia 2020 r.

1. Przedmiot opinii prawnej

1.1. Przedmiotem niniejszej opinii prawnej (dalej jako "**Opinia**") są prawne aspekty bezpieczeństwa poczty elektronicznej w praktyce wykonywania zawodu radcy prawnego w kontekście obowiązku zachowania tajemnicy zawodowej oraz ochrony danych osobowych.

1.2. Dla sporządzenia niniejszej Opinii podstawę stanowiły następujące akty prawne:

a) Ustawa z dnia 6 lipca 1982 r. o radcach prawnych (t.j. Dz.U. z 2020 r. poz. 75, dalej jako „**URP**" lub „**ustawa o radcach prawnych**");

b) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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) (Dz. Urz. UE z 2016 r. Nr L 119/1, dalej jako „**RODO**");

c) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 r. poz. 1781, dalej jako „**UODO**").

1.3. Opinię przygotowano również z uwzględnieniem następujących dokumentów:

a) Załącznik do uchwały Nr 3/2014 Nadzwyczajnego Krajowego Zjazdu Radców Prawnych z dnia 22 listopada 2014 r. - Kodeks Etyki Radcy Prawnego (dalej jako „**KERP**");

b) Uchwała nr 94/IX/2015 KRRP z 13.6.2015 r. w sprawie Regulaminu wykonywania zawodu radcy prawnego (dalej jako „**Regulamin wykonywania zawodu radcy prawnego**");

c) Uchwała nr 54/2009 Naczelnej Rady Adwokackiej z 12 września 2009 roku w sprawie Regulaminu wykonywania zawodu w kancelarii indywidualnej lub spółkach[39] (dalej jako „**Regulamin wykonywania zawodu adwokata**");

d) Opinia Generalnego Inspektora Ochrony Danych Osobowych w sprawie bezpieczeństwa danych przekazywanych przy użyciu poczty elektronicznej, dalej „**Opinia GIODO**";

e) Wytyczne niemieckiej Federalnej Izby Adwokackiej co do używania usługi Microsoft Office 365 Cloud (niem. *Hinweise zum Umgang mit Microsoft Office 365 Cloud aus datenschutzrechtlicher Sicht*)[40], dalej jako "**Wytyczne Niemieckiej Federalnej Izby Adwokackiej**";

[39] Dostępne pod adresem: http://www.nra.pl/admin/wgrane_dokumenty/Regulamin_wykonywania_zawodu_tekst_jednolity.pdf.

[40] Hinweise zum Umgang mit Microsoft Office 365 Cloud aus datenschutzrechtli- cher Sicht – Stand: November 2019, dostępne pod adresem: https://www.brak.de/w/files/02_fuer_anwaelte/datenschutz/hinweise-zum-umgang-mit-office-365-cloud_stand-25-11-2019.pdf.

f) Wytyczne Federalnej Izby Doradców Podatkowych co do komunikacji za pomocą e-maili (niem. *Hinweise zur E-Mail-Kommunikation*)[41], dalej „**Wytyczne Niemieckiej Federalnej Izby Doradców Podatkowych**";

g) Zasady zawodowe adwokatów w Niemczech (niem. Berufsordnung für Rechtsanwälte), dalej „**Niemieckie zasady zawodowe adwokatów**";

h) Wytyczne Rady Adwokackiej Anglii i Walii w sprawie używania poczty elektronicznej (ang. The General Bar Council's Email Guidelines)[42], dalej „**Wytyczne Rady Adwokackiej Anglii i Walii dot. poczty elektronicznej**";

i) Wytyczne Rady Adwokackiej Anglii i Walii w sprawie bezpieczeństwa informacji (ang. The General Bar Council's Guidelines on Information Security)[43], dalej „**Wytyczne Rady Adwokackiej Anglii i Walii dot. bezpieczeństwa informacji**";

j) Opinia 477R Stałego Komitetu do spraw etyki i odpowiedzialności zawodowej Amerykańskiego Stowarzyszenia Prawników w sprawie zabezpieczenia przekazywania poufnych informacji dotyczących klientów (ang. American Bar Association Standing Committee On Ethics and Professional Responsibility – Formal Opinion 477R)[44], dalej jako „**Wytyczne ABA**";

k) Modelowe Zasady Etyki Zawodowej Amerykańskiego Stowarzyszenia Prawników (ang. American Bar Association Model Rules of Professional Conduct)[45], dalej „**Modelowe Zasady Etyki Zawodowej ABA**".

1.4. Opinia podzielona została na następujące zagadnienia:

- Na wstępie przedstawione zostaną przyczyny ochrony komunikacji z użyciem poczty elektronicznej i zagrożenia związane z korzystaniem przez radców prawnych z poczty.
- Następnie omówione będzie to jak wiadomości są przesyłane są poprzez pocztę elektroniczną oraz w jaki sposób mogą być zabezpieczane. Do tych sposobów zabezpieczenia odnoszą się w części wytyczne wskazane w dalszej części Opinii.
- W dalszej kolejności poddane analizie zostaną krajowe i zagraniczne przepisy oraz wytyczne dotyczące bezpieczeństwa przesyłania za pośrednictwem poczty elektronicznej informacji objętych tajemnicą zawodową oraz ochrona danych osobowych.
- W następnej części będą ogólnie przedstawione najczęściej występujące zagrożenia bezpieczeństwa informacji związane z korzystaniem z poczty elektronicznej. W tej części wskazane będą też podstawowe przykładowe środki

---

[41] Dostępne pod adresem: https://www.bstbk.de/export/sites/standard/de/ressourcen/Dokumente/04_presse/publikationen/02_steuerrecht_rechnungslegung/55_2019-01-29_BStBK-Hinweise_zur_E-Mail-Kommunikation.pdf.

[42] The Bar Council Email Guidelines, dostępne pod adresem: https://www.barcouncilethics.co.uk/wp-content/uploads/2017/10/Email-guidelines-for-the-Bar-1.pdf.

[43] Dokument dostępny pod adresem: https://www.barcouncilethics.co.uk/wp-content/uploads/2019/11/Information-Security-1.pdf.

[44] Dostępne pod adresem: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf.

[45] Dokument dostępny pod adresem: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents/.

zabezpieczające, które można stosować w związku z korzystaniem z poczty elektronicznej.

- Na końcu przedstawione będą rekomendacje co do przesyłania przez radców prawnych za pośrednictwem poczty elektronicznej informacji objętych tajemnicą zawodową lub danych osobowych, w tym co do sposobów zabezpieczenia oraz ustalania ich z klientem.

2. Prawne przyczyny ochrony komunikacji z użyciem poczty elektronicznej i zagrożenia związane z korzystaniem przez radców prawnych z poczty elektronicznej

2.1. Zasady korzystania z poczty elektronicznej powinny wynikać ze spoczywających na radcy prawnym obowiązków ochrony informacji związanych z wykonywaniem zawodu. Wspomniane obowiązki odnoszą się do zachowania **poufności** informacji, ale także jej **integralności** i **dostępności.**

2.2. Podstawowe obowiązki w tym zakresie wynikają z prawnych zasad:

- ochrony tajemnicy zawodowej (tajemnicy radcy prawnego),
- ochrony danych osobowych.

2.3. Jednym z podstawowych warunków wykonywania przez radcę prawnego swojego zawodu jest obowiązek zachowania przez niego tajemnicy zawodowej, która dotyczy wszystkiego, o czym dowiedział się w związku z udzielaniem pomocy prawnej (art. 3 ust. 3 ustawy o radcach prawnych). Obowiązek zachowania w poufności (sekrecie) informacji przez radcę prawnego nie ogranicza się do zakazu ujawniania tajnych informacji, ale rozciąga się na potrzebę zabezpieczenia procesu komunikacji z klientem i innymi osobami, tak aby nieuprawnione osoby trzecie nie miały dostępu do tych informacji. Powyższy obowiązek dotyczy każdego sposobu komunikacji – i tradycyjnej, i elektronicznej. Za naruszenie tajemnicy może zostać uznane już takie zaniechanie, poprzez brak zabezpieczeń komunikacji lub ich niewystarczający poziom, który tylko stworzy możliwość dostępu do poufnych informacji nieuprawnionym podmiotom.

2.4. Jeżeli przedmiotem przetwarzanych przez radcę prawnego informacji są dane osobowe to niezależnie od obowiązku zachowania tajemnicy zawodowej znajdą zastosowanie przepisy o ochronie danych osobowych, w tym przede wszystkim RODO. W jednej z podstawowych zasad określonych w tym akcie wymaga się, aby dane osobowe były przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo tych danych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność") (art. 5 ust.1 lit. f) RODO). Wspomniane środki powinny zostać również przedsięwzięte w procesach przekazywania (komunikacji) danych osobowych.

2.5. Wspomniane powyżej atrybuty bezpieczeństwa informacji – poufność, integralność i dostępność – określa się w następujący sposób (zgodnie z normą ISO 27001):

a) poufność oznacza właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom,

b) integralność oznacza właściwość zapewnienia dokładności i kompletności aktywów (zasobów),

c) dostępność oznacza właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.

2.6. Zagrożenia dotyczące powyższych atrybutów bezpieczeństwa informacji w odniesieniu do korzystania z poczty elektronicznej można przedstawić następująco:

a) Zagrożenie dotyczące poufności informacji przesyłanych pocztą elektroniczną może polegać na tym, że osoba nieuprawniona zapozna się z treścią wiadomości e-mail przesyłanej radcę prawnego lub do niego.

b) Zagrożenie dotyczące integralności informacji przesyłanych pocztą elektroniczną może polegać na tym, że osoba nieuprawniona „przechwyci" wiadomość przesyłaną przez radcę prawnego lub do niego i zmieni treść tej wiadomości.

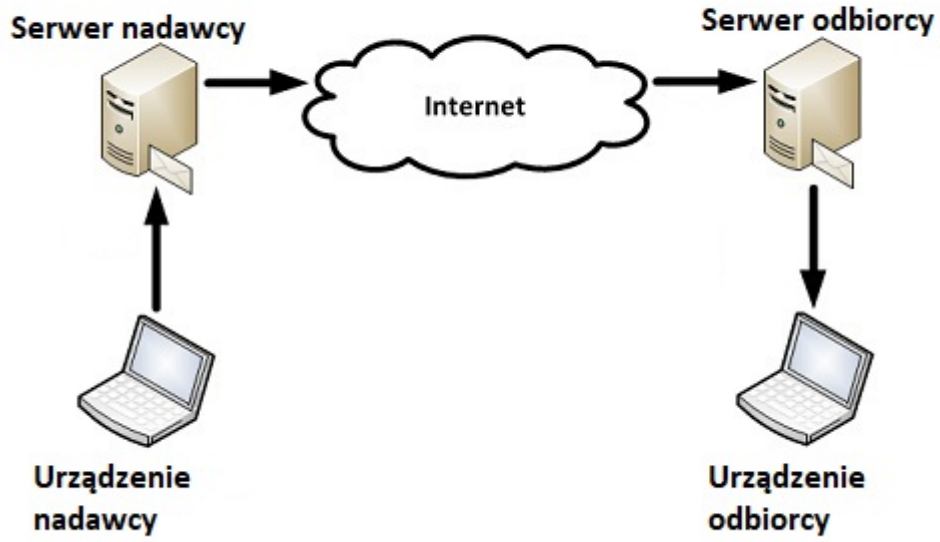
c) Zagrożenie dotyczące dostępności informacji przesyłanych pocztą elektroniczną może polegać na tym, że osoba nieuprawniona „przechwyci" wiadomość i w ogóle nie dojdzie ona do adresata, albo dojdzie z opóźnieniem.

3. Sposób działania poczty elektronicznej i zabezpieczenia komunikacji z jej użyciem

3.1. Na wstępie należy ogólnie przedstawić, jak przesyłane są wiadomości poprzez pocztę elektroniczną oraz w jaki sposób wiadomości te mogą być zabezpieczane. Ma to istotne znaczenie, ponieważ niektóre wytyczne omówione w dalszej części Opinii (pkt 4) wprost odnoszą się do niektórych sposobów zabezpieczenia wiadomości e-mail.

3.2. Poniższy schemat w bardzo uproszczony sposób ilustruje drogę, którą wiadomość e-mail „przebywa" ze skrzynki pocztowej nadawcy do skrzynki pocztowej odbiorcy[46].

[46] Bardziej szczegółowe omówienie sposobu działania poczty elektronicznej: Simple Mail Transfer Protocol, [w:] Wikipedia, Wolna encyklopedia, artykuł dostępny pod adresem: https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol (dostęp: 16.03.2020).



3.3. Wiadomość e-mail jest najpierw przesyłana z urządzenia nadawcy (np. komputera, telefonu, tabletu) do serwera pocztowego nadawcy. Następnie wiadomość jest przesyłana z serwera nadawcy do serwera odbiorcy. Na tym etapie wiadomość e-mail przekazywana jest przez sieć Internet, między różnymi urządzeniami w tej sieci, aby trafić do serwera odbiorcy. Następnie wiadomość e-mail przekazywana jest z serwera odbiorcy na urządzenie odbiorcy.

3.4. W początkowej fazie rozwoju poczty elektronicznej wiadomości e-mail były przesyłane między poszczególnymi urządzeniami otwartym tekstem, tj. bez żadnych zabezpieczeń. Obecnie istnieje jednak kilka sposobów zabezpieczania wiadomości e-mail[47].

3.5. W niniejszej opinii zostaną w sposób podstawowy przedstawione następujące przypadki:

- brak zabezpieczeń (wysyłanie wiadomości e-mail otwartym tekstem);
- szyfrowanie podczas przesyłania przy użyciu protokołu TLS (SSL);
- szyfrowanie treści wiadomości end-to-end;
- szyfrowanie załączników jako inna metoda zabezpieczania treści.

3.6. Warto dodać, że powyższe sposoby zabezpieczenia wiadomości e-mail są wskazane w niektórych wytycznych dotyczących bezpieczeństwa poczty elektronicznej w kontekście ochrony tajemnicy zawodowej (omówionych w pkt 4 poniżej).

3.7. Brak zabezpieczenia wiadomości e-mail oznacza, że treść wiadomości (a także ewentualnego załącznika) jest wysyłana otwartym tekstem. Należy wziąć pod uwagę, że wiadomość e-mail przesyłana jest między wieloma urządzeniami w sieci Internet zanim dotrze do swojego adresata. Wysyłanie wiadomości e-mail bez żadnych zabezpieczeń porównywane jest do wysyłania kartki pocztowej, którą każdy, kto ma do

[47] Email encryption [w:] Wikipedia, Wolna encyklopedia, artykuł dostępny pod adresem: https://en.wikipedia.org/wiki/Email_encryption (dostęp: 16.03.2020).

niej dostęp, może przeczytać[48] (chociaż w przypadku wiadomości e-mail oczywiście niezbędne są do tego odpowiednie umiejętności techniczne). W związku z brakiem jakiegokolwiek zabezpieczenia jej treści, pojawia się ryzyko naruszenia poufności, a nawet integralności wiadomości.

3.8. Szyfrowanie podczas przesyłania (czy też szyfrowanie na poziomie transmisji; ang. *Transport-level encryption*) przy pomocy protokołu TLS (SSL) oznacza, że wiadomość jest zaszyfrowana podczas jej przesyłania[49]. Innymi słowy, tworzone jest bezpieczne połączenie między urządzeniem nadawcy a urządzeniem odbiorcy wiadomości e-mail w czasie jej przesyłania. Należy jednak zaznaczyć, że nie jest to szyfrowanie treści wiadomości. Szyfrowanie podczas przesyłania stanowi zabezpieczenie przed utratą poufności lub integralności wiadomości. Przełamanie tego zabezpieczenia jest oczywiście możliwe (znane są ataki przeciwko TLS), jednak uzyskanie dostępu do treści wiadomości lub jej zmiana jest duża bardziej utrudniona niż w sytuacji braku zabezpieczeń.

3.9. Należy jednak zaznaczyć, że stosowanie szyfrowania podczas przesyłania zależy od ustawień serwera nadawcy oraz serwera odbiorcy. Tylko jeżeli zarówno serwer nadawcy, jak i serwer odbiorcy mają włączoną obsługę protokołu TLS, to utworzone będzie szyfrowane połączenie na czas wysyłania wiadomości. Oznacza to, że jeżeli tylko serwer nadawcy obsługuje protokół TLS, a serwer odbiorcy go nie obsługuje, to wiadomość e-mail zostanie wysłana bez zabezpieczeń. Nie ma możliwości wcześniejszego sprawdzenia, czy serwer odbiorcy obsługuje protokół TLS. Możliwe jest takie ustawienie serwera nadawcy, aby nie wysyłał on wiadomości e-mail jeżeli serwer odbiorcy nie obsługuje protokołu TLS (tj. nie da zapewnić się szyfrowania podczas przesyłania). Jednakże w praktyce nie korzysta się z tego rozwiązania, ponieważ doprowadziłoby do tego, że część wiadomości e-mail nie zostałaby dostarczona do adresatów. W związku z tym nadawca nie ma pewności, czy jego wiadomość została zaszyfrowana podczas transportu, chyba że wcześniej uzyskał od odbiorcy zapewnienie, że serwer odbiorcy obsługuje protokół TLS (i zapewnienie to było prawdziwe).

3.10. Najbardziej zaawansowanym sposobem zabezpieczenia wiadomości e-mail jest szyfrowanie ich treści metodą end-to-end[50]. W tym przypadku treść wiadomości jest szyfrowana przez jej nadawcę i w postaci zaszyfrowanej jest wysyłana do odbiorcy, który jako jedyny może ją odszyfrować i odczytać. Innymi słowy, tylko nadawca i odbiorca mogą odczytać treść wiadomości e-mail – dostępu do treści nie mają podmioty takie jak dostawcy usługi poczty e-mail. Taki rodzaj szyfrowania zapewnia najlepszą ochronę poufności i integralności wiadomości. Jednakże stosowanie szyfrowania end-to-end wymaga wdrożenia tego rozwiązania zarówno przez nadawcę, jak i odbiorcę. Jako że szyfrowanie end-to-end opiera się o kryptografię klucza

[48] Email privacy [w:] Wikipedia, Wolna encyklopedia, artykuł dostępny pod adresem: https://en.wikipedia.org/wiki/Email_privacy (dostęp: 15.04.2020).

[49] Bardziej szczegółowe omówienie dotyczące działania protokołów TLS/SSL: Transport Layer Security, [w:] Wikipedia, Wolna encyklopedia, artykuł dostępny pod adresem: https://en.wikipedia.org/wiki/Transport_Layer_Security (dostęp: 16.03.2020).

[50] Bardziej szczegółowe omówienie dotyczące szyfrowania end-to-end: End-to-end encryption, [w:] Wikipedia, Wolna encyklopedia, artykuł dostępny pod adresem: https://en.wikipedia.org/wiki/End-to-end_encryption (dostęp: 16.03.2020).

publicznego[51], to aby wysyłać szyfrowane w ten sposób wiadomości, konieczna byłaby wymiana kluczy publicznych między nadawcą a adresatem[52]. Szyfrowanie end-to-end nie jest szeroko stosowane w ramach usługi poczty e-mail.

3.11. Innym sposobem zabezpieczenia treści wiadomości e-mail, niezależnym od powyższych rozwiązań, jest zaszyfrowanie załącznika do wiadomości e-mail i przesłanie go w takiej formie do odbiorcy. W takim przypadku hasło (klucz) do zaszyfrowanego pliku może być przekazany odbiorcy innym bezpiecznym kanałem (np. telefonicznie, przez SMS)[53]. Zastosowanie szyfrowania załącznika stanowi dodatkowe zabezpieczenie w sytuacji, w której nie ma pewności, czy wiadomość e-mail jest szyfrowana podczas przesyłania (szyfrowanym połączeniem). Jak wskazano powyżej, o ile nadawca nie uzyska od odbiorcy informacji, czy serwer odbiorcy obsługuje protokół TLS, to nadawca nie ma pewności, czy wysłana przez niego wiadomość e-mail będzie szyfrowana podczas przesyłania.

4. Analiza krajowych i zagranicznych przepisów oraz wytycznych dotyczących bezpieczeństwa poczty elektronicznej w kontekście ochrony tajemnicy zawodowej i danych osobowych

Wprowadzenie

4.1. W tej części analizie zostaną poddane krajowe oraz zagraniczne regulacje prawne, zarówno powszechnie obowiązujące, jak i o charakterze soft law, które odnoszą się do kwestii bezpieczeństwa poczty elektronicznej w kontekście ochrony tajemnicy zawodowej i danych osobowych. W szczególności chodzi tutaj o bezpieczeństwo przesyłania informacji objętych tajemnicą zawodową oraz danych osobowych za pośrednictwem poczty elektronicznej. Analiza ta ma na celu omówienie stanu prawnego obecnie obowiązującego w Polsce oraz rozwiązań przyjętych w tym zakresie w innych państwach.

4.2. Ze względu na fakt, że w ramach korzystania z poczty elektronicznej przez radców prawnych najczęściej będzie dochodziło do przekazywania informacji objętych tajemnicą zawodową radcy prawnego lub informacji mających charakter danych

[51] Bardziej szczegółowe omówienie dotyczące kryptografii klucza publicznego: Public-key cryptography, [w:] Wikipedia, Wolna encyklopedia, artykuł dostępny pod adresem: https://en.wikipedia.org/wiki/Public-key_cryptography (dostęp: 16.03.2020).
[52] Opinia GIODO, s. 3.
[53] Opinia GIODO, s. 2.

osobowych, nacisk zostanie położony na regulacje dotyczące ochrony tajemnicy zawodowej oraz przepisy o ochronie danych osobowych.

4.3. W tym zakresie zidentyfikowane zostały dwa kluczowe obszary problemowe, które zostaną bardziej szczegółowo omówione poniżej: **(1) wybór dostawcy poczty elektronicznej,** oraz **(2) przesyłanie informacji objętych tajemnicą zawodową lub danych osobowych za pośrednictwem poczty elektronicznej, w tym komunikacja z klientem.**

4.4. Na wstępie należy wskazać, że na poziomie krajowym brak jest jak dotąd przepisów prawa powszechnie obowiązującego, jak i przepisów wewnątrzkorporacyjnych, które wprost określałyby zasady bezpieczeństwa poczty elektronicznej wykorzystywanej przez radców prawnych. W szczególności kwestii tych nie reguluje ani ustawa o radcach prawnych, ani Kodeks Etyki Radcy Prawnego, ani Regulamin wykonywania zawodu radcy prawnego. Należy się zatem odnieść do przepisów tych regulacji dotyczących tajemnicy zawodowej radcy prawnego.

Regulacje dotyczące tajemnicy zawodowej

4.5. Na podstawie art. 3 ust. 3 URP, radcowie prawni są zobowiązani do **zachowania w tajemnicy** wszystkiego, o czym dowiedzieli się w związku z udzieleniem pomocy prawnej. Obowiązek zachowania tajemnicy zawodowej nie może być ograniczony w czasie, a radca prawny nie może być zwolniony z obowiązku zachowania tajemnicy zawodowej co do faktów, o których dowiedział się udzielając pomocy prawnej lub prowadząc sprawę.

4.6. **Kodeks Etyki Radcy Prawnego** precyzuje zakres obowiązku zachowania tajemnicy zawodowej radcy prawnego (art. 15 – 24) i stanowi, że radca prawny jest obowiązany zachować w tajemnicy wszystkie informacje dotyczące klienta i jego spraw, ujawnione radcy prawnemu przez klienta bądź uzyskane w inny sposób w związku z wykonywaniem przez niego jakichkolwiek czynności zawodowych, niezależnie od źródła tych informacji oraz formy i sposobu ich utrwalenia. Tajemnica zawodowa obejmuje również wszelkie tworzone przez radcę prawnego dokumenty oraz korespondencję radcy prawnego z klientem i osobami uczestniczącymi w prowadzeniu sprawy - powstałe dla celów związanych ze świadczeniem pomocy prawnej. Tajemnicą zawodową objęte są także informacje ujawnione radcy prawnemu przed podjęciem przez niego czynności zawodowych, jeżeli z okoliczności sprawy wynika, że ujawnienie nastąpiło dla potrzeb świadczenia pomocy prawnej i uzasadnione było oczekiwaniem, że radca prawny będzie ją świadczył.

4.7. Objęte tajemnicą będą zatem informacje przekazane w formie ustnej, w postaci papierowej lub elektronicznej, utrwalone za pomocą wszelkich nośników informacji(np. na płycie CD, DVD, pendrivie, ale również w systemie teleinformatycznym, w tym udostępnione w chmurze), a także przesyłane w jakikolwiek sposób[54].

4.8. Zgodnie z art. 23 **Kodeksu Etyki,** radca prawny obowiązany jest zabezpieczyć przed niepowołanym ujawnieniem wszelkie informacje objęte tajemnicą zawodową, niezależnie od ich formy i sposobu utrwalenia. Zgodnie z Kodeksem, dokumenty i nośniki zawierające informacje poufne należy przechowywać w sposób chroniący je

[54] L. Korczak, Komentarz do art. 3 URP, [w:] T. Scheffler (red.), Ustawa o radcach prawnych. Komentarz, 2018, Legalis.

przed zniszczeniem, zniekształceniem lub zaginięciem, natomiast dokumenty i nośniki przechowywane w formie elektronicznej powinny być objęte odpowiednią kontrolą dostępu oraz zabezpieczeniem systemu przed zakłóceniem działania, uzyskaniem nieuprawnionego dostępu lub utratą danych. Radca prawny zobowiązany jest jednocześnie do kontrolowania dostępu osób współpracujących do takich dokumentów i nośników.

4.9. Regulacja ta ogranicza się zatem do zobowiązania radcy prawnego do:

1) zabezpieczenia informacji przed ich ujawnieniem,
2) przechowywania nośników informacji w sposób zabezpieczający przed zniszczeniem, zniekształceniem bądź zaginięciem,
3) zapewnienia kontroli dostępu do dokumentów przechowywanych w formie elektronicznej,
4) zabezpieczenia systemu informatycznego przed zakłóceniem działania, uzyskaniem nieuprawnionego dostępu lub utratą danych,
5) zapewnienia sobie kontroli dostępu do dokumentów i nośników dla osób współpracujących[55].

4.10. Art. 23 KERP uzupełnia **§ 10 Regulaminu wykonywania zawodu radcy prawnego,** które razem uważane są za instrukcję postępowania z dokumentami w formie tradycyjnej oraz danymi przechowywanymi w formie elektronicznej[56].

4.11. Zgodnie z § 10 Regulaminu wykonywania zawodu radcy prawnego, radca prawny powinien zapewnić należyte warunki przechowywania dokumentów związanych z prowadzeniem sprawy, zabezpieczając je przed zniszczeniem, zaginięciem i przed dostępem osób niepowołanych. Sposób postępowania z dokumentami związanymi z prowadzeniem sprawy po zakończeniu zlecenia powinien być ustalony z klientem, a w braku takiego ustalenia oraz w przypadku niezgłoszenia przez klienta żądania zwrotu powierzonych mu dokumentów, związanych z prowadzeniem sprawy, radca prawny po wykonaniu zlecenia powinien wezwać klienta do odbioru tych dokumentów. Może on jednak może zachować kopie tych dokumentów.

4.12. Dla porównania warto się w tym kontekście odnieść do Regulaminu wykonywania zawodu adwokata. Zgodnie z **§ 5 Regulaminu wykonywania zawodu adwokata**, korespondencja elektroniczna prowadzona przez adwokata musi być zabezpieczona przed dostępem osób spoza kancelarii lub spółki, co nie stoi na przeszkodzie zlecaniu czynności administrowania systemem informatycznym przez osoby trzecie.

4.13. Stosownie do § 7, adwokat jest zobowiązany postępować z informacjami objętymi tajemnicą zawodową adwokata (informacje poufne) w sposób uniemożliwiający zapoznanie się z nimi osobom trzecim. W działalności zawodowej adwokat lub spółka, w której adwokat wykonuje zawód **stosuje fizyczne i logiczne zabezpieczenia, które zapewniają bezpieczeństwo systemu informatycznego i danych klientów w stopniu wynikającym z rozwoju techniki w danym czasie**. W szczególności system

[55] L. Korczak, Komentarz do art. 23 KERP, [w:] T. Scheffler (red.), Kodeks Etyki Radcy Prawnego. Komentarz, 2016, Legalis.
[56] L. Korczak, Komentarz do art. 23 KERP, [w:] T. Scheffler (red.), Kodeks Etyki Radcy Prawnego. Komentarz, 2016, Legalis.

informatyczny służący do przechowywania informacji poufnych powinien być zabezpieczony przed (i) działaniem oprogramowania, którego celem jest zakłócenie działania lub uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz (ii) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

4.14. W dalszej części opinii omówione będą przepisy i rekomendacje (soft law) dotyczące korzystania przez radców prawnych (lub przedstawicieli innych regulowanych zawodów prawniczych) z poczty elektronicznej i jej bezpieczeństwa, z uwzględnieniem wyboru dostawcy poczty elektronicznej oraz przesyłania za pośrednictwem poczty elektronicznej informacji objętych tajemnicą zawodową lub danych osobowych.

Wybór dostawcy poczty elektronicznej

Regulacje krajowe – powszechnie obowiązujące

4.15. W prawie krajowym brak jest przepisów, które wprost wymagałyby spełnienia określonych warunków dotyczących bezpieczeństwa przez dostawców poczty elektronicznej dla kancelarii radców prawnych.

Ustawa o radcach prawnych

4.16. Należy jednak zwrócić uwagę, że zgodnie z art. 3 ust. 3 URP „*Radca prawny jest obowiązany zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzieleniem pomocy prawnej".* Należy z tego wnioskować, że narzędzia wybierane i stosowane przez radców prawnych powinny również zapewnić zachowanie tajemnicy zawodowej.

RODO

4.17. Ponadto na gruncie RODO obowiązek zachowania poufności danych osobowych należy wywodzić z art. 5 ust. 1 lit. f) RODO, zgodnie z którym dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

4.18. **Zasada zapewnienia bezpieczeństwa danych osobowych** została skonkretyzowana w art. 32 RODO, zgodnie z którym administrator uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o równych prawdopodobieństwie wystąpienia i wadze, wdraża odpowiednie środki technicznej i organizacyjne, aby zapewnić bezpieczeństwo odpowiadające ryzyku. Oznacza to, że RODO nie dostarcza administratorowi wykazu środków bezpieczeństwa, które powinien stosować w poczcie elektronicznej, ponieważ zabezpieczenia powinny być dobrane adekwatnie do ryzyka naruszenia praw lub wolności osób fizycznych. W art. 32 RODO określono wyłącznie przykładowe środki bezpieczeństwa:

- pseudonimizacja i szyfrowanie danych osobowych;

- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

4.19. **W kontekście korzystania z poczty elektronicznej szczególne znaczenie ma szyfrowanie treści wiadomości e-mail lub szyfrowanie podczas przesyłania przy użyciu protokołu TLS, o czym mowa szerzej powyżej w pkt 3 Opinii.**

4.20. **Przepisy o ochronie danych osobowych dopuszczają sytuację, w której administrator zleca zewnętrznemu dostawcy usług przetwarzanie danych osobowych, np. dostawcy usługi poczty elektronicznej.** Na administratorze ciąży obowiązek wyboru odpowiedniego podmiotu przetwarzającego, co wynika z art. 28 ust. 1 RODO „*Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług* ***takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych****, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą."* Pojęcie „wystarczające gwarancje" ma charakter nieostry, ocenny i wpisuje się w koncepcję ochrony danych osobowych opartej na ryzyku. Poziom wystarczających gwarancji może być różny i uzależniony od tego, jakie dane podlegają przetwarzaniu (zwykłe albo wrażliwe), w jakiej ilości, w jakim celu, za pomocą jakich technik[57].

4.21. Należy przyjąć, że kancelaria radcy prawnego lub spółka[58] jest administratorem w rozumieniu art. 4 pkt 7 RODO[59], a dostawca usługi poczty elektronicznej jest podmiotem przetwarzającym w rozumieniu art. 4 pkt 8 RODO, gdyż przetwarza dane osobowe znajdujące się w wiadomościach w imieniu administratora. Administrator powinien korzystać wyłącznie z takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Obowiązek ten został wyjaśniony bardziej szczegółowo w motywie 81 do RODO, w którym wskazano, że administrator powinien korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje co do **wiedzy fachowej, wiarygodności i zasobów**. Administrator powinien sprawdzić powyższe gwarancje przed powierzeniem podmiotowi przetwarzającemu czynności przetwarzania. Jako wiedzę fachową należy rozumieć doświadczenie dostawcy w świadczeniu usług związanych z przetwarzaniem danych, powołanie inspektora ochrony danych lub – gdy nie jest to wymagane – koordynatora ds. ochrony danych czy też przeszkolenie pracowników z zakresu ochrony danych i bezpieczeństwa

[57] Komentarz do art. 28 [w:] M. Sakowska-Baryła (red.), Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, Warszawa 2018

[58] Chodzi o sytuację, w której radca prawny wykonuje zawód w spółce, której wyłącznym przedmiotem działalności jest świadczenie pomocy prawnej, w formach określonych w art. 8 ust. 1 URP. W takiej sytuacji administratorem danych osobowych jest właśnie spółka.

[59] Szerzej na temat statusu administratora radcy prawnego zob.: I. Małobęcka-Szwast, Status adwokata i radcy prawnego w procesie przetwarzania danych osobowych w świetle RODO i przepisów prawa krajowego, dodatek do Monitora Prawniczego nr 22/2018 „Przepisy prawa uzupełniające RODO". Aktualne problemy prawnej ochrony danych osobowych 2018; X. Konarski, G. Sibiga, D. Nowak, K. Syska, I. Małobęcka-Szwast, K. Barszczewska-Mazur, Ogólne rozporządzenie o ochronie danych (RODO). Poradnik dla radców prawnych i adwokatów, 2019.

informacji. O wiarygodności dostawcy będzie w przyszłości świadczyć stosowanie zatwierdzonego kodeksu postępowania (art. 40 RODO) lub zatwierdzonego mechanizmu certyfikacji (art. 42 RODO). Jako zasoby należy natomiast rozumieć wdrożenie polityk i procedur związanych z ochroną danych, wdrożenie zasad bezpieczeństwa informacji zgodnie z normami ISO 27000, wdrożenie środków technicznych i organizacyjnych takich jak szyfrowanie podczas przesyłania lub szyfrowanie treści wiadomości e-mail, o czym szerzej w pkt 3 Opinii powyżej. Dlatego też te przesłanki mogą być również wzięte pod uwagę przez radcę prawnego przy wyborze dostawcy.

4.22. To na kancelarii radcy prawnego lub spółce, w której wykonuje on zawód jako administratorze danych ciąży również obowiązek wykazania, że przed wyborem dostawcy dokonano analizy pod kątem zapewniania przez niego tych gwarancji.

4.23. Następnie administrator zgodnie z art. 28 ust. 3 RODO jest zobowiązany do zawarcia umowy powierzenia przetwarzania danych, która powinna określać zasady wykonywania przez dostawcę obowiązków, o których mowa w art. 28 ust. 3 RODO. Należy zwrócić uwagę, że na podstawie umowy powierzenia podmiot przetwarzający jest zobowiązany m.in. **do współpracy z administratorem w zakresie bezpieczeństwa danych:**

- zgodnie z art. 28 ust. 3 lit. c) RODO podmiot przetwarzający jest zobowiązany podejmować wszelkie środki wymagane na mocy art. 32 RODO, czyli w zakresie bezpieczeństwa danych osobowych,
- zgodnie z art. 28 ust. 3 lit. f) RODO podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36 RODO, czyli w zakresie zapewnienia bezpieczeństwa danych osobowych, zarządzania naruszeniami ochrony danych oraz przeprowadzania oceny skutków dla ochrony danych,
- zgodnie z art. 28 ust. 3 lit. h) RODO podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

4.24. Przy wyborze dostawcy poczty elektronicznej należy również zwrócić uwagę, czy dane osobowe będą przetwarzane na terenie Europejskiego Obszaru Gospodarczego, czy też poza nim, a to ze względu na restrykcje z rozdziału V RODO określającego zasady transferu danych poza EOG. Jeżeli zgodnie z umową dostawca poczty elektronicznej mógłby przechowywać zawartość skrzynki pocztowej radcy prawnego poza EOG, to należy sprawdzić, czy w danym państwie zapewniony jest odpowiedni poziom ochrony lub zapewniono odpowiednie zabezpieczenia w rozumieniu art. 45-47 RODO.

Krajowe regulacje korporacyjne i soft law

4.25. **Ani Kodeks Etyki Radcy Prawnego ani Regulamin wykonywania zawodu radcy prawnego nie określają wprost wymogów jakie powinna spełniać poczta elektroniczna, z której korzysta radca prawny, w tym jakie wymogi powinien spełniać zewnętrzny dostawca poczty elektronicznej**. Zgodnie z wcześniej przywołanym art. 15 ust. 1 KERP *„Radca prawny jest obowiązany zachować w tajemnicy wszystkie informacje dotyczące klienta i jego spraw, ujawnione radcy*

prawnemu przez klienta bądź uzyskane w inny sposób w związku z wykonywaniem przez niego jakichkolwiek czynności zawodowych, niezależnie od źródła tych informacji oraz formy i ***sposobu ich utrwalenia*** *(tajemnica zawodowa*)". Ponadto zgodnie z art. 23 KERP *„Radca prawny obowiązany jest zabezpieczyć przed niepowołanym ujawnieniem wszelkie informacje objęte tajemnicą zawodową,* ***niezależnie od ich formy i sposobu utrwalenia.*** *Dokumenty i nośniki zawierające informacje poufne należy przechowywać w sposób chroniący je przed zniszczeniem, zniekształceniem lub zaginięciem. Dokumenty i nośniki przechowywane w formie elektronicznej powinny być objęte odpowiednią kontrolą dostępu oraz zabezpieczeniem systemu przed zakłóceniem działania, uzyskaniem nieuprawnionego dostępu lub utratą danych. Radca prawny powinien kontrolować dostęp osób współpracujących do takich dokumentów i nośników."*

4.26. Jako że powyższe przepisy zobowiązują radcę prawnego do zabezpieczenia informacji objętych tajemnicą zawodową przed ujawnieniem niezależnie od ich formy i sposobu utrwalenia, to należy z tego wnioskować, że ponosi on również odpowiedzialność za wybór zewnętrznego dostawcy narzędzi informatycznych, w tym poczty elektronicznej, który w praktyce będzie zapewniał zabezpieczenia umożliwiające skuteczną ochronę informacji objętych tajemnicą zawodową. Zobowiązania do objęcia kontrolą dostępu, zabezpieczeniem przed zakłóceniem działania, uzyskaniem nieuprawnionego dostępu lub utratą danych w naszej opinii powinno również dotyczyć wybieranych przez radców prawnych rozwiązań służących do komunikacji, w tym poczty elektronicznej i jej dostawców. W praktyce oznacza to konieczność szczegółowej analizy umów lub regulaminów świadczenia usług (które w przypadku dużych dostawców są zazwyczaj nie do negocjowania) przed wyborem właściwego rozwiązania.

4.27. Dodatkowo należy zwrócić uwagę, że zgodnie z § 5 ust. 4 Regulaminu wykonywania zawodu adwokata *„Korespondencja elektroniczna musi być zabezpieczona przed dostępem osób spoza kancelarii lub spółki, co nie stoi na przeszkodzie zlecaniu czynności administrowania systemem informatycznym przez osoby trzecie. Postanowienia § 1 ust. 16 stosuje się odpowiednio."* Postanowienie to wprowadza obowiązek po stronie adwokata do zabezpieczenia dostępu do poczty elektronicznej, jednocześnie dopuszczając administrowanie pocztą elektroniczną przez osoby trzecie, ale przy zapewnieniu zachowania tajemnicy adwokackiej. Regulacja ta nie wprowadza natomiast kryteriów, które powinna spełniać taka osoba trzecia zaangażowana przez adwokata. Takie kryteria można pośrednio wywodzić z § 7 ust. 8 zd. 2 Regulaminu wykonywania zawodu adwokata, zgodnie z którym *„W szczególności system informatyczny służący do przechowywania informacji poufnych powinien być zabezpieczony przed (i) działaniem oprogramowania, którego celem jest zakłócenie działania lub uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz (ii) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej".* Ponadto § 7 ust. 9 Regulaminu wykonywania zawodu adwokata wprowadza obowiązek, aby informacje poufne przechowywane w systemie informatycznym były zabezpieczane przez wykonywanie kopii zapasowych zbiorów danych elektronicznych, które powinny być przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.

Regulacje zagraniczne – powszechnie obowiązujące

4.28. W jurysdykcjach podlegających badaniu (tj. Niemcy, Austria, Wielka Brytania, Stany Zjednoczone) nie zidentyfikowano regulacji prawnych o charakterze powszechnie obowiązującym, które odnosiłyby się do zagadnienia wyboru dostawcy poczty elektronicznej przez osoby wykonujące zawody prawnicze.

4.29. W przypadku jurysdykcji z EOG osoby wykonujące zawody prawnicze powinny stosować RODO w zakresie przetwarzania danych osobowych przesyłanych poprzez pocztę elektroniczną.

Zagraniczne regulacje korporacyjne i soft law

4.30. Zgodnie z § 2 ust. 2 Niemieckich zasad zawodowych adwokatów *„Obowiązek zachowania poufności wymaga od adwokata podjęcia środków organizacyjnych i technicznych niezbędnych do ochrony poufności klienta, które są adekwatne do ryzyka i uzasadnione dla zawodu prawnika.* ***Środki techniczne są do tego wystarczające, o ile spełniają wymagania przepisów dotyczących ochrony danych osobowych”.***

4.31. Warto zwrócić uwagę, że w zakresie środków technicznych służących do zachowania ochrony poufności klienta dokument ten odsyła do przepisów o ochronie danych osobowych oraz wskazuje, że środki techniczne powinny być adekwatne do ryzyka, co sprowadza się do stosowania podejścia opartego na ryzyku.

4.32. Wskazówek co do wyboru dostawców dostarczają również Wytyczne ABA, zgodnie z którymi to na prawniku ciąży obowiązek nadzoru nad osobami świadczącymi na rzecz kancelarii usługi o charakterze nieprawniczym, co ma również zastosowanie w przypadku outsourcingu usług komunikacji elektronicznej. Przy wyborze takiego dostawcy należy brać pod uwagę w szczególności: referencje, doświadczenie i reputację, rodzaj świadczonych usług, stosowanie przez dostawcę polityk i protokołów bezpieczeństwa, zasady zatrudniania, warunki umowy dotyczące ochrony informacji klientów, dostępność środków prawnych w przypadku naruszenia umowy przez dostawcę, ramy prawne i etyczne co do poufności informacji w jurysdykcjach, w których usługi mogą być częściowo świadczone. Następnie na prawniku ciąży obowiązek monitorowania bezpieczeństwa świadczonych przez dostawcę usług, jak również dokonywania okresowo ponownej oceny powyższych czynników ze względu na zmieniające się okoliczności oraz technologie, aby poufność danych była zachowana[60].

4.33. Jeżeli prawnik nie jest w stanie samodzielnie ocenić zabezpieczeń służących zachowaniu poufności danych klientów, to należy zaangażować innego prawnika, eksperta lub dokształcić się w tym zakresie.

Ryzyka prawne związane z korzystaniem z nieodpłatnych („darmowych”) skrzynek poczty elektronicznej przez radcę prawnego

4.34. Na tle powyższych uwag należy też zwrócić uwagę na ryzyka prawne związane z korzystaniem przez radców prawnych z nieodpłatnych („darmowych”) skrzynek poczty elektronicznej. Trzeba zwrócić szczególną uwagę na te warunki świadczenia usług, których stosowanie w odniesieniu do radcy prawnego mogłoby spowodować, że nie spełniałby on ciążących na nim obowiązków dotyczących ochrony tajemnicy

[60] Wytyczne ABA, s. 10.

zawodowej lub ochrony danych osobowych. Do takich warunków należą w szczególności:

- postanowienie, że dostawca usług poczty elektronicznej będzie wykorzystywać informacje znajdujące się w skrzynce poczty elektronicznej do własnych celów (np. statystycznych) – w takiej sytuacji może dojść do naruszenia poufności informacji znajdujących się w skrzynce (co byłoby również naruszeniem art. 5 ust. 1 lit. f) RODO);
- postanowienie, że po określonym czasie nielogowania do poczty elektronicznej przez użytkownika, zawartość skrzynki elektronicznej zostanie usunięta – w takiej sytuacji może dojść do naruszenia dostępności informacji znajdujących się w skrzynce (co byłoby również naruszeniem art. 32 ust. 1 RODO);
- warunki świadczenia usług nie spełniają wymogów dotyczących umowy powierzenia przetwarzania określonych w art. 28 ust. 3 RODO (patrz pkt 4.23 powyżej) – w takiej sytuacji doszłoby do naruszenia wskazanego wyżej przepisu RODO.

Przesyłanie informacji objętych tajemnicą zawodową lub danych osobowych za pośrednictwem poczty elektronicznej, w tym komunikacja z klientem

Regulacje krajowe – powszechnie obowiązujące

4.35. Na poziomie krajowym brak jest jak dotąd powszechnie obowiązujących przepisów prawa, które wprost określałyby wymagane zabezpieczenia poczty elektronicznej, czy zasady ustalania tych zabezpieczeń z klientem i komunikowania mu zagrożeń związanych z korespondencją prowadzoną drogą elektroniczną. W szczególności kwestii tych nie reguluje ustawa o radcach prawnych.

4.36. Należy jednak wskazać, że na gruncie RODO na administratorze danych (w tym przypadku radcy prawnym lub spółce, w której wykonuje on zawód) ciąży obowiązek doboru zabezpieczeń (środków technicznych lub organizacyjnych) adekwatnych do ryzyka naruszenia praw lub wolności osób fizycznych, tak aby zapewnić odpowiednie bezpieczeństwo przetwarzanych danych osobowych (art. 5 ust. 1 lit. f), art. 24 i art. 32 RODO). W związku z tym radca prawny lub spółka powinna przeprowadzić szacowanie ryzyka zgodnie z powyższymi przepisami i ustalić odpowiednie środki techniczne i organizacyjne w celu zabezpieczenia danych osobowych, w tym danych osobowych wysyłanych za pośrednictwem poczty elektronicznej.

4.37. W praktyce jednak, ze względu na fakt, że radca prawny lub spółka najprawdopodobniej będzie korzystała w tym zakresie z dostawców zewnętrznych, obowiązek ten będzie się przekładał na wybór odpowiedniego dostawcy poczty elektronicznej, co szerzej zostało omówione w podrozdziale „Wybór dostawcy poczty elektronicznej" powyżej.

Krajowe regulacje korporacyjne i soft law

4.38. Na poziomie krajowym nie istnieją również szczegółowe wytyczne samorządu radców prawnych. Ani Kodeks Etyki Radcy Prawnego, ani Regulamin wykonywania zawodu radcy prawnego nie określają, jakie zabezpieczenia w zakresie korzystania z poczty elektronicznej ma stosować radca prawny, ani jak owe zabezpieczenia mają być dobierane. Regulacje te nie odnoszą się również do kwestii uzgadniania z klientem

zabezpieczeń poczty elektronicznej w przypadku przesyłania informacji objętych tajemnicą zawodową, czy informowania klienta o stosowanych przez radcę prawnego zabezpieczeniach lub o zagrożeniach dla poufności i integralności informacji związanych z korzystaniem z poczty elektronicznej.

4.39. Kodeks Etyki Radcy Prawnego jedynie ogólnie stanowi, że radca prawny obowiązany jest zabezpieczyć przed niepowołanym ujawnieniem wszelkie informacje objęte tajemnicą zawodową, niezależnie od ich formy i sposobu utrwalenia (art. 23). Z KERP wynika zalecenie, aby dokumenty i nośniki przechowywane w formie elektronicznej były objęte odpowiednią kontrolą dostępu.

4.40. Do kwestii tych odnosi się również **Regulamin wykonywania zawodu adwokata**, zgodnie z którym adwokat jest zobowiązany postępować z informacjami objętymi tajemnicą zawodową adwokata (informacje poufne) w sposób uniemożliwiający zapoznanie się z nimi osobom trzecim. W działalności zawodowej adwokat lub spółka, w której adwokat wykonuje zawód zobowiązana jest do **stosowania fizycznych i logicznych zabezpieczeń, które zapewniają bezpieczeństwo systemu informatycznego i danych klientów w stopniu wynikającym z rozwoju techniki w danym czasie**. W szczególności system informatyczny służący do przechowywania informacji poufnych powinien być zabezpieczony przed (i) działaniem oprogramowania, którego celem jest zakłócenie działania lub uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz (ii) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej. W Regulaminie wskazano, że choć korespondencja elektroniczna prowadzona przez adwokata musi być zabezpieczona przed dostępem osób spoza kancelarii lub spółki, to nie stoi to na przeszkodzie zlecaniu czynności administrowania systemem informatycznym przez osoby trzecie (§ 7 Regulaminu wykonywania zawodu adwokata). W Regulaminie brak jest jednak bardziej szczegółowych rozwiązań dotyczących zabezpieczeń poczty elektronicznej, które miałyby być wdrażane przez adwokatów.

Regulacje zagraniczne – powszechnie obowiązujące

4.41. W jurysdykcjach podlegających badaniu (tj. Niemcy, Austria, Wielka Brytania, Stany Zjednoczone) nie zidentyfikowaliśmy regulacji prawnych o charakterze powszechnie obowiązującym, które odnosiłyby się do zagadnienia zabezpieczeń poczty elektronicznej wykorzystywanej w korespondencji między prawnikiem a klientem.

4.42. Warto jednak w tym kontekście zwrócić uwagę na wprowadzenie w Niemczech przez Federalną Izbę Adwokacką tzw. specjalnej elektronicznej skrzynki pocztowej dla adwokatów (niem. besonderes elektronisches Anwaltspostfach, w skrócie beA)[61]. Wymóg jej wprowadzenia nakłada na **Federalną Izbę Adwokacką** § 31a niemieckiej ustawy o adwokatach (niem. Bundesrechtsanwaltsordnung)[62].

[61] Niemieckie określenie „der Anwalt" można tłumaczyć zarówno jako adwokat, prawnik lub też pełnomocnik.

[62] Bundesrechtsanwaltsordnung, treść ustawy dostępna pod adresem: https://www.gesetze-im-internet.de/brao/__31a.html.

4.43. Stosowanie specjalnej elektronicznej skrzynki adwokackiej w Niemczech jest obowiązkowe w określonym w ustawie zakresie[63]. Od dnia 1 stycznia 2018 r. członkowie izb adwokackich mają bowiem bierny obowiązek korzystania ze skrzynki na podstawie §31a ust. 6 niemieckiej ustawy o adwokatach. Tym samym **obowiązkiem każdego adwokata zrzeszonego w Izbie jest regularne sprawdzanie w skrzynce, czy otrzymał on jakiekolwiek wiadomości**. Obowiązek aktywnego korzystania ze skrzynki – w zależności od prawa danego kraju związkowego – wchodzi w życie w 2020 r., a najpóźniej musi zostać on zrealizowany do dnia 1 stycznia 2022 r.[64]. Aktywne korzystanie ze skrzynki polegać ma w szczególności na dostarczaniu za jej pomocą dokumentów drogą elektroniczną do sądu. Co istotne, wiele kancelarii w Niemczech stosuje beA również do komunikacji z klientami, niemniej nie ma to charakteru obligatoryjnego.

Zagraniczne regulacje korporacyjne i soft law

4.44. Kwestia bezpieczeństwa poczty elektronicznej jako narzędzia przekazywania informacji objętych tajemnicą zawodową, w tym komunikacji zawodowego prawnika z klientem została dostrzeżona przez prawnicze korporacje w kilku państwach. W niniejszej części omówione będą: (i) Wytyczne Rady Adwokackiej Anglii i Walii dot. bezpieczeństwa informacji; (ii) Wytyczne Rady Adwokackiej Anglii i Walii dot. poczty elektronicznej; (iii) Niemieckie zasady zawodowe adwokatów; (iv) Wytyczne Niemieckiej Federalnej Izby Doradców Podatkowych; oraz (v) Wytyczne ABA.

4.45. **Rada Adwokacka Anglii i Walii** (the General Council of the Bar) w Wytycznych dotyczących bezpieczeństwa informacji zauważa, że komunikacja za pomocą poczty elektronicznej wiąże się z potencjalnym ryzykiem w zakresie bezpieczeństwa.

4.46. Rada zaleca przyjęcie określonych rozwiązań, które w założeniu mają minimalizować to ryzyko. Należą do nich: szyfrowanie podczas przesyłania wiadomości, jeżeli przekazuje się szczególnie wrażliwe informacje tą drogą lub jeżeli klient wymaga szyfrowania korespondencji. W takich przypadkach należy uzgodnić z klientem metodę szyfrowania.

4.47. W przypadku **szyfrowania treści załącznika**, Rada odradza wysyłanie hasła wymaganego do odszyfrowania załącznika w tym samym mailu, co załącznik, jako sprzeczne z celem szyfrowania.

4.48. Rada postuluje również zachowanie ostrożności podczas korzystania z funkcji „**autouzupełniania**" oferowanej przez niektóre systemy poczty e-mail, aby uniknąć przypadkowego wybrania nieprawidłowego adresu poczty elektronicznej. Zaleca jednocześnie zachowanie ostrożności przy korzystaniu z funkcji kopii (DW) i ukrytej kopii (UDW), aby upewnić się, że wiadomość nie zostanie wysłana do niewłaściwego odbiorcy. Jednocześnie Rada rekomenduje, aby listy zawierające wcześniej używane numery telefonów, faksów i adresy e-mail były na bieżąco aktualizowane.

4.49. **Rada Adwokacka Anglii i Walii** w Wytycznych dotyczących poczty elektronicznej podkreśla, że adwokaci powinni być świadomi potrzeby zapewnienia odpowiedniego bezpieczeństwa korespondencji elektronicznej i wszelkich załączników do nich.

---

[63] beA: Das besondere elektronische Anwaltspostfach, https://brak.de/fuer-anwaelte/bea-das-besondere-elektronische-anwaltspostfach/.

[64] *Ibidem*.

Wskazuje, że od adwokatów oczekuje się przedsięwzięcia rozsądnych środków ostrożności w celu zapewnienia bezpieczeństwa swoich komputerów i wszelkich innych środków komunikacji, z których korzystają, gdy zajmują się sprawami reprezentowanego klienta. Rada odradza stosowanie programów do śledzenia poczty e-mail tj. takich programów, które umożliwiają zautomatyzowane otrzymywanie informacji, czy i kiedy odbiorca otrzymał, otworzył wiadomość i załączniki, jak również stosowania adresu e-mail służącego do komunikacji z klientami w celach prywatnych (np. jako loginu do mediów społecznościowych).

4.50. Rada wprost rekomenduje, aby kancelarie korzystały z systemów, które:

- zapewniają funkcję pobierania (i automatycznego odszyfrowywania) zaszyfrowanej poczty przychodzącej;
- umożliwiają kancelarii zaszyfrowanie treści wiadomości e-mail, jeżeli klient tego wymaga.

4.51. W ocenie Rady, kancelarie powinny bezpiecznie przechowywać prywatne klucze kryptograficzne i posiadać politykę zarządzania tymi kluczami. W przypadkach kancelarii, Rada rekomenduje wdrożenie pisemnych zasad dotyczących wykorzystywania poczty elektronicznej.

4.52. Środki, które można podjąć w celu zarządzania zagrożeniami bezpieczeństwa, obejmują regularne kontrole logów e-mail pracowników pod kątem naruszenia bezpieczeństwa oraz rejestrowanie dostępu do prywatnych obszarów sieci kancelarii.

4.53. Rada zaleca również, aby korespondencja elektroniczna była opatrzona automatycznym ostrzeżeniem, że informacje w niej zawarte mają poufny charakter (są objęte tajemnicą zawodową) i są przeznaczone wyłącznie dla odbiorcy. Chociaż automatyczne ostrzeżenia o poufności nie nakładają prawnie wiążących obowiązków na niezamierzonego odbiorcę, można się spodziewać, że wielu odbiorców się do nich zastosuje. Do ostrzeżenia można również dodać link odsyłający do polityki prywatności kancelarii.

4.54. W Niemczech na szczególną uwagę w omawianym zakresie zasługują Zasady zawodowe adwokatów. Od 1 stycznia 2020 roku w życie weszło w życie nowe brzmienie § 2 ust. 2 Niemieckich zasad zawodowych adwokatów, poprzez które Federalna Izba Adwokacka chciała odpowiedzieć na potencjalne ryzyko dla utrzymania tajemnicy korespondencji pomiędzy adwokatem a klientem związane z wykorzystywaniem niezaszyfrowanych wiadomości email[65].

4.55. Zgodnie z brzmieniem § 2 ust. 2 Niemieckich zasad zawodowych adwokatów, obowiązek zachowania tajemnicy wymaga od adwokata podjęcia środków organizacyjnych i technicznych niezbędnych do ochrony tajemnicy klienta, które są adekwatne do ryzyka i uzasadnione dla zawodu adwokata. Środki techniczne są wystarczające, o ile spełniają wymagania określone w przepisach dotyczących ochrony danych osobowych. Inne środki techniczne muszą również odpowiadać najnowszemu stanowi techniki. W każdym przypadku dozwolone jest stosowanie pomiędzy adwokatem a klientem elektronicznego lub innego środka komunikacji, z którym związane jest ryzyko dla poufności tej komunikacji, jeżeli klient wyrazi na jego

[65] Anwaltsblatt, Verschwiegenheit: § 2 BORA zu E-Mails de Anwalts an Mandanten ab 2020, https://anwaltsblatt.anwaltverein.de/de/anwaeltinnen-anwaelte/anwaltspraxis/verschwiegenheit-neue-bora-norm-zu-e-mails-an-mandanten?full=1#panel-der-neue-2-bora-im-wortlaut.

stosowanie zgodę. O zgodzie klienta można mówić, jeśli klient zasugeruje lub zacznie stosować taki kanał komunikacji i będzie kontynuował jego używanie po tym, jak adwokat odniesie się przynajmniej ogólnie do ryzyka bez podawania szczegółów technicznych.

4.56. Warto zauważyć, że przepis ten nie dotyczy wyłącznie poczty elektronicznej, ale jakiegokolwiek innego środka komunikacji, który może wywoływać ryzyko dla poufności korespondencji (zasady zakładają w tym zakresie neutralność technologiczną). Należy zwrócić uwagę, że zgodnie z Niemieckimi zasadami zawodowymi adwokatów, jeżeli klient wyrazi zgodę na dany środek komunikacji, którego stosowanie niesie ze sobą ryzyko dla poufności, to wyklucza to naruszenie zasad wykonywania zawodu adwokata. Jeżeli klient dalej będzie używał danego środka komunikacji w kontaktach z adwokatem, po otrzymaniu uwag adwokata co do ryzyk w tym zakresie, to domniemywa się, że klient wyraził zgodę na ów środek komunikacji[66].

4.57. Pewnych wskazówek w zakresie bezpieczeństwa poczty elektronicznej dostarczają również Wytyczne Niemieckiej Federalnej Izby Doradców Podatkowych co do komunikacji za pomocą e-maili. Warto zauważyć, że doradcy podatkowi w Niemczech, podobnie jak adwokaci, również zobowiązani są do zachowania tajemnicy zawodowej. Federalna Izba Doradców Podatkowych wśród możliwych sposobów zabezpieczenia korespondencji wyszczególnia: szyfrowanie podczas przysyłania (ang. *transport encryption*, niem. *Transportverschlüsselung*) oraz tzw. szyfrowanie end-to end (*Die Ende-zu-Ende-Verschlüsselung*).

4.58. Izba wskazuje, że szyfrowanie podczas przesyłania (szyfrowanie TLS/SSL; ten rodzaj zabezpieczenia został szerzej omówiony w pkt 3.88-3.99 Opinii) jest co do zasady standardową metodą szyfrowania w ruchu e-mail. Zdaniem Izby szyfrowanie poczty w trakcie przesyłania jest wystarczającym środkiem zapewniającym poufność. Doradca podatkowy musi więc upewnić się, że wiadomość e-mail jest szyfrowana podczas przesyłania, oraz że serwery dostawców usługi poczty e-mail, z której korzystają doradca podatkowy oraz jego klient znajdują się w Niemczech. Izba doradza, aby w celu zapewnienia większego poziomu bezpieczeństwa komunikacji zabezpieczyć załączniki do danej wiadomości e-mail hasłem.

4.59. Ponadto, w ocenie Izby, szyfrowanie end-to-end (szyfrowanie treści wiadomości; omówione szerzej w pkt 3.1010 Opinii) nie jest co do zasady niezbędne do zapewnienia odpowiedniego poziomu bezpieczeństwa. Jak wspomniano wyżej, dzięki zastosowaniu tej metody tylko nadawcy i odbiorcy mogą odczytać treść wiadomości e-mail, jeśli mają niezbędny klucz.

4.60. Izba wskazuje również, że zgoda klienta na komunikację za pomocą niezabezpieczonych środków komunikacji jest wystarczająca z punktu widzenia zasad wykonywania zawodu. Jednakże Izba zwraca uwagę również na fakt, że w przypadku danych wrażliwych (na przykład dokumentów zawierających oświadczenie podatkowe, rozliczenie roczne) jest niezbędne, aby doradca podatkowy uzyskał odrębną konkretną zgodę na ich niezabezpieczone przesłanie. W przypadku danych osobowych osób

[66] Anwaltsblatt, Verschwiegenheit: § 2 BORA zu E-Mails des Anwalts an Mandanten ab 2020, https://anwaltsblatt.anwaltverein.de/de/anwaeltinnen-anwaelte/anwaltspraxis/verschwiegenheit-neue-bora-norm-zu-e-mails-an-mandanten?full=1#panel-der-neue-2-bora-im-wortlaut.

trzecich (np. dane małżonka) taką zgodę należy uzyskać bezpośrednio od tych osób trzecich.

4.61. Izba rekomenduje, aby sposób oraz zasady komunikacji elektronicznej z klientem określić już na etapie zawierania umowy. Przykładowe porozumienie dotyczące sposobu komunikacji elektronicznej znajduje się w załączniku do wytycznych[67].

4.62. Wytyczne dotyczące zabezpieczania przekazywania informacji poufnych wydało także Amerykańskie Stowarzyszenie Prawników. Wytyczne ABA odnoszą się w tym kontekście do Modelowych Zasad Etyki Zawodowej ABA, z których wynika obowiązek zachowania poufności informacji związanych z prowadzeniem spraw klienta. Zgodnie z pkt 1.6 Modelowych Zasad Etyki Zawodowej ABA, prawnik powinien przedsięwziąć rozsądne środki, aby przeciwdziałać przypadkowemu lub nieuprawnionemu ujawnieniu lub nieuprawnionemu dostępowi do informacji związanych z prowadzeniem spraw klienta.

4.63. Z Wytycznych ABA wynika, że prawnik może co do zasady prowadzić korespondencję z klientem z wykorzystaniem środków komunikacji elektronicznej, nie naruszając przy tym zasad etyki zawodowej, jeżeli dołożył on rozsądnych starań, aby zapobiec nieumyślnemu lub nieuprawnionemu dostępowi do treści wiadomości. Jednakże prawnik może być zobowiązany do podjęcia specjalnych środków bezpieczeństwa w celu ochrony przed przypadkowym lub nieuprawnionym ujawnieniem informacji związanych z prowadzeniem spraw klienta, jeżeli wymaga tego umowa z klientem lub przepisy prawa lub gdy charakter informacji wymaga zastosowania wyższego stopnia bezpieczeństwa.

4.64. Zgodnie z Wytycznymi prawnicy powinni dokonywać oceny, czy w danym przypadku konieczne jest zastosowanie szczególnych zabezpieczeń komunikacji elektronicznej. Zależy to przede wszystkim od charakteru (wrażliwości) przekazywanych informacji, prawdopodobieństwa ujawnienia informacji, kosztu i trudności związanych z wdrożeniem dodatkowych zabezpieczeń. W niektórych przypadkach wymagane mogą być szczególne środki zabezpieczające, takie jak szyfrowanie.

4.65. Ponadto w Wytycznych ABA zalecane jest ustalenie z klientem sposobów zabezpieczenia informacji przekazywanych drogą elektroniczną, a dotyczących spraw klienta. Przykładowo, może to być szyfrowanie podczas przesyłania lub zabezpieczenie załącznika hasłem.

4.66. Jednocześnie w Wytycznych ABA wskazano, że używanie nieszyfrowanej poczty elektronicznej jest dopuszczalne do porozumiewania się z klientem w sprawach bieżących, gdzie nie dochodzi do przekazywania informacji poufnych.

4.67. Podsumowując, krajowe ani zagraniczne przepisy powszechnie obowiązujące nie odnoszą się do kwestii korzystania przez radców prawnych (lub przedstawicieli innych regulowanych zawodów prawniczych) z poczty elektronicznej w komunikacji z klientem, ani do sposobów jej zabezpieczania. Natomiast niektóre prawnicze korporacje i stowarzyszenia odniosły się do tej kwestii w wydawanych przez siebie rekomendacjach i zbiorach zasad. W omówionych powyżej dokumentach wskazano następujące rekomendacje:

[67] Wytyczne Niemieckiej Federalnej Izby Doradców Podatkowych, s.6.

- informowanie klienta o ryzykach związanych z przesyłaniem informacji poufnych drogą elektroniczną i przesyłanie ich bez dodatkowych zabezpieczeń tylko za wyraźną lub dorozumianą zgodą klienta;
- ustalanie z klientem sposobów zabezpieczenia informacji przesyłanych między prawnikiem a klientem pocztą elektroniczną;
- dokonywanie oceny, jakie zabezpieczenia powinny być zastosowane w danym przypadku, biorąc pod uwagę między innymi charakter (wrażliwość) przekazywanych informacji;
- w niektórych wytycznych wprost mowa jest o konkretnych metodach zabezpieczenia informacji podczas przesyłania pocztą elektroniczną, takich jak szyfrowanie podczas przesyłania (z zastosowaniem TLS), zabezpieczenie przesyłanego załącznika hasłem, szyfrowanie treści wiadomości.

4.68. Niektóre z omawianych wytycznych odnoszą się do zasad komunikacji z klientem, a inne – bardziej ogólnie – do zasad przekazywania pocztą elektroniczną informacji dotyczących prowadzenia spraw klienta (informacji objętych tajemnicą zawodową). W naszej opinii zasady zabezpieczania informacji objętych tajemnicą zawodową przesyłanych poczty elektronicznej powinny odnosić się nie tylko do komunikacji z klientem, ale do każdego przypadku przesyłania informacji objętych tajemnicą zawodową (informacji dotyczących prowadzenia spraw klienta) za pośrednictwem poczty elektronicznej. Może się bowiem zdarzyć tak, że informacje są przesyłane do współpracującego prawnika czy też do innego pełnomocnika klienta. W szczególności w przypadku, gdy sposoby zabezpieczania informacji przesyłanych pocztą elektroniczną zostały ustalone z klientem, to te sposoby powinny być stosowane w każdym przypadku wysyłania informacji dotyczących spraw tego klienta.

4.69. Wydaje się, że powyższa zasada stosowania zabezpieczeń informacji przekazywanych pocztą elektroniczną, w szczególności gdy sposoby zabezpieczenia zostały ustalone z klientem, powinny także dotyczyć przekazywania przez radcę prawnego informacji objętych tajemnicą zawodową do organów władzy publicznej (w przypadkach, w których możliwe jest wnoszenie pism za pośrednictwem poczty elektronicznej). Jednakże może okazać 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). W takich przypadkach rekomendowane jest zastosowanie innych środków ostrożności, takich jak dokładne sprawdzenie adresu e-mail odbiorcy. Odradzane jest też zbędne wysyłanie pocztą elektroniczną korespondencji, która została lub ma być przekazana do organu w inny sposób (np. przez ePUAP, pocztą tradycyjną, osobiście).

5. Najczęstsze zagrożenia dla bezpieczeństwa informacji w związku z korzystaniem z poczty elektronicznej oraz podstawowe środki zabezpieczające

5.1. Niezależnie od powyżej przedstawionych problemów dotyczących poufności przesyłanej korespondencji, poczta elektroniczna może być źródłem zagrożenia dla całego systemu informatycznego, z którego korzysta radca prawny oraz informacji w nim zawartych. W niniejszej części będą przedstawione najczęściej występujące zagrożenia bezpieczeństwa informacji związane z korzystaniem z poczty elektronicznej. Chodzi tu o zagrożenia, które generalnie wiążą się z korzystaniem z poczty elektronicznej i nie odnoszą się wyłącznie do poufności przesyłanych informacji stanowiących tajemnicę zawodową lub dane osobowe. W Opinii zwracamy uwagę na takie generalne zagrożenia oraz wskazujemy podstawowe środki zabezpieczające, ponieważ ma to wpływ na bezpieczeństwo korzystania z poczty elektronicznej.

5.2. W związku z tym w niniejszej części wskazane będą typowe zagrożenia dla dostępności, integralności, jak również poufności informacji występujące w przypadku korzystania z poczty elektronicznej oraz przedstawione będą przykładowe środki bezpieczeństwa w celu unikania omawianych zagrożeń.

Zagrożenia dla bezpieczeństwa informacji w związku z korzystaniem z poczty elektronicznej

5.3. Przy obecnym rozwoju technologii dynamicznie zmieniają się zagrożenia w związku z korzystaniem z internetu i poczty elektronicznej. Obecnie najczęściej występujące zagrożenia mogące mieć znaczenie dla korzystania z poczty elektronicznej to *phishing*, *malware* oraz *ransomware*. Zagrożenia te są opisane poniżej. Należy jednak pamiętać, że istnieją także inne rodzaje zagrożeń związane zarówno z korzystaniem z poczty elektronicznej, jak i dotyczące ogólnie pojmowanego bezpieczeństwa informacji.

5.4. **Phishing** jest to metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej (socjotechniki)[68], tj. stosowaniu środków psychologicznych i metod manipulacji mających na celu wyłudzenie określonych informacji.

5.5. W 2019 roku phishing polegał w szczególności:

- na wysyłaniu wiadomości przez podszywających się pod dostawców w celu wyłudzeniu płatności,
- wyłudzanie poświadczeń do kont (hasło, login),

[68] Bardziej szczegółowe informacje o metodzie phishinu: Phishing, [w:] Wikipedia, Wolna encyklopedia, artykuł dostępny pod adresem: https://pl.wikipedia.org/wiki/Phishing (dostęp: 15.04.2020).

- wysyłanie fałszywych faktur na adres e-mail przez podmioty podszywające się pod dostawców telekomunikacyjnych,
- wysyłanie do klientów banku informacji o nieautoryzowanym logowaniu w celu nakłonienia do podania danych do logowania na fałszywej stronie internetowej[69].

5.6. **Malware** to ogół programów mających szkodliwe działanie w stosunku do systemu komputerowego lub jego użytkownika (zbitka słów *malicious* „złowrogi, złośliwy" i *software* „oprogramowanie")[70]. W związku z korzystaniem z poczty elektronicznej należy zwracać uwagę na załączniki i linki w wiadomościach od nieznanych lub niebudzących zaufania nadawców, których otworzenie może zainicjować zainstalowanie złośliwego oprogramowania, które może spowodować zarówno utratę poufności danych, jak i ich integralności.

5.7. **Ransomware** to typ szkodliwego oprogramowania, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych (często poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego (zbitka słów *ransom* „okup" i software „oprogramowanie")[71].

5.8. Przykładem ataku ransomware było zaszyfrowanie danych na komputerach Urzędu Gminy w Kościerzynie w 2019 r., które spowodowało utratę dostępności danych na klika tygodni. Atak ransomware może być również efektem udanego ataku phishingowego. Dla przykładu, Klinika dziecięca „Budzik" otrzymała e-mail z żądaniem zapłaty za fakturę i zainfekowanym linkiem. W wyniku ataku komputery Kliniki zostały zaszyfrowane, co doprowadziło do utraty dostępności danych u uniemożliwiło pracę placówki [72].

Podstawowe środki bezpieczeństwa

5.9. Poniżej przedstawione są przykładowe środki bezpieczeństwa, które powinien stosować radca prawny w związku z korzystaniem z poczty elektronicznej. Poza przedstawionymi środkami należy także stosować środki w celu przeciwdziałania innym zagrożeniom bezpieczeństwa informatycznego, chociażby związane z bezpieczeństwem fizycznym sprzętu informatycznego lub bezpieczeństwem sieci.

5.10. Radca prawny powinien każdorazowo sprawdzać adres e-mail nadawcy, w tym zastanowić się, czy nadawca jest mu znany, czy otrzymywał od tego nadawcy już wcześniej inne wiadomości oraz czy spodziewał się otrzymać tę wiadomość. Jeżeli nadawca jest mu znany (mecenas XYZ), radca prawny powinien sprawdzić, czy dany adres e-mail odpowiada adresowi e-mail, z którego otrzymywał on poprzednie wiadomości od tego nadawcy. Często fałszywe adresy e-mail mogą różnić się w niewielkim zakresie od prawdziwych adresów e-mail (np. @oirpwarszawa.com zamiast @oirpwarszawa.pl).

5.11. Radca prawny powinien zwracać uwagę na treść wiadomości, zwłaszcza jeżeli otrzymana wiadomość pochodzi od nieznanego nadawcy. Należy zachować szczególną ostrożność klikając w linki lub otwierając załączniki zamieszczone w

[69] Raport CERT Orange Polska za rok 2019, s.13-15
[70] Złośliwe oprogramowanie, [w:] Wikipedia, Wolna encyklopedia, artykuł dostępny pod adresem: https://pl.wikipedia.org/wiki/Z%C5%82o%C5%9Bliwe_oprogramowanie (dostęp: 15.04.2020).
[71] Ransomware: [w:] Wikipedia, Wolna encyklopedia, artykuł dostępny pod adresem: https://pl.wikipedia.org/wiki/Ransomware (dostęp: 15.04.2020).
[72] Raport CERT Orange Polska za rok 2019, s.13-15

wiadomości, w szczególności gdy wiadomość zawiera błędy gramatyczne lub ortograficzne, wygląda na tłumaczoną za pomocą translatora lub tytuł wiadomości i nazwa załącznika nie ma sensu.

5.12. Radca prawny powinien zachować w poufności hasła do poczty elektronicznej i regularnie je zmieniać (np. raz na 3 miesiące). W celu zapewnienia odpowiedniego bezpieczeństwa, hasło nie powinno być oczywiste i łatwe do odgadnięcia przez osoby trzecie. Hasło do służbowej poczty elektronicznej powinno być inne niż hasło do innych skrzynek poczty elektronicznej, sklepów internetowych czy portali społecznościowych. W tym zakresie rozwiązaniem, które można rozważyć, jest korzystanie z tzw. menadżera haseł – narzędzia, które służy do generowania, bezpiecznego przechowywania i automatycznego wprowadzania haseł do poczty elektronicznej oraz innych stron internetowych. Ponadto, jeżeli dostawca poczty elektronicznej zapewnia taką możliwość, zalecane jest korzystanie z uwierzytelniania dwuskładnikowego (weryfikacji dwuetapowej), która polega na wykorzystaniu w trakcie logowania dodatkowego etapu weryfikacji użytkownika (np. wpisanie jednorazowego kodu wysłanego przez usługodawcę za pomocą wiadomości SMS oprócz logowania za pomocą hasła użytkownika).

5.13. Radca prawny nie powinien wykorzystywać służbowego adresu e-mail do wysyłania i odbierania wiadomości prywatnych.

5.14. Radca prawny powinien pamiętać o bieżących aktualizacjach systemu operacyjnego oraz oprogramowania antywirusowego, które powinno również służyć do ochrony poczty elektronicznej.

5.15. Służbowy adres e-mail nie powinien być wykorzystywany jako login do portali internetowych wykorzystywanych w celach prywatnych, w tym w szczególności portali społecznościowych.

5.16. Radca prawny nie powinien przesyłać wiadomości służbowych na prywatne konto poczty elektronicznej.

5.17. Pozostali pracownicy kancelarii również powinni stosować się do powyższych zasad bezpieczeństwa. Pracownicy i współpracownicy kancelarii powinni zostać odpowiednio przeszkoleni, a szkolenia z zakresu ochrony danych osobowych i bezpieczeństwa informacji powinny być przeprowadzane okresowo. Należy pamiętać, że w przypadku wymienionych zagrożeń to człowiek jest często „najsłabszym ogniwem”.

5.18. Zalecane jest wprowadzenie w kancelarii polityki korzystania z poczty elektronicznej, która powinna uwzględniać powyższe kwestie, lub zamieszczenie tych zasad w polityce bezpieczeństwa informacji. Oprócz tego zwracamy uwagę, że elementem całościowej polityki bezpieczeństwa informacji (polityki ochrony danych) w kancelarii powinny być zasady reagowania na incydenty bezpieczeństwa informacji i naruszenia ochrony danych osobowych. Ze względu na zmiany w technologiach zalecane jest również regularne aktualizowanie tego typu dokumentów.

6. Wnioski i rekomendacje

Wybór dostawcy

6.1. Radca prawny wybierając dostawcę poczty elektronicznej powinien kierować się koniecznością zachowania tajemnicy zawodowej zgodnie z ustawą o radcach prawnych, Kodeksem Etyki Radcy Prawnego i Regulaminem wykonywania zawodu radcy prawnego.

6.2. Do wyboru dostawcy poczty elektronicznej znajdują zastosowanie przepisy o ochronie danych osobowych, w szczególności:

a) zasada integralności i poufności (art. 5 ust. 1 lit. f) RODO,

b) zasady bezpieczeństwa danych osobowych (art. 32 RODO),

c) dokonanie wyboru dostawcy usługi poczty elektronicznej zgodnie z art. 28 ust. 1 RODO i motywem 81 RODO,

d) zawarcie umowy powierzenia przetwarzania (art. 28 RODO) uwzględniającej odpowiednie zabezpieczenia poczty elektronicznej, w tym szyfrowanie wiadomości.

6.3. Jeżeli radca prawny nie posiada wiedzy pozwalającej na ocenę bezpieczeństwa poszczególnych narzędzi, to zalecane jest skorzystanie z pomocy innego radcy prawnego, eksperta w zakresie bezpieczeństwa informacji lub też pogłębienie wiedzy w tym zakresie samodzielnie.

6.4. Zalecane jest ostrożne korzystanie z „darmowych" skrzynek poczty elektronicznej, w tym dokładne sprawdzenie warunków świadczenia usług pod kątem zgodności z przepisami prawa i zasadami bezpieczeństwa informacji, o czym szerzej w pkt 4.34 Opinii.

Sposoby ochrony przesyłanych informacji, w tym kryptograficzna ochrona informacji

6.5. Radca prawny powinien sprawdzić i być świadomy tego w jaki sposób zabezpieczane są wiadomości e-mail, które są wysyłane z jego skrzynki poczty elektronicznej.

6.6. Sposobami zabezpieczania wiadomości e-mail mogą być:

- Szyfrowanie podczas przesyłania przy użyciu protokołu TLS (ang. *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 przesłanie go w takiej formie do odbiorcy. Hasło (klucz) do zaszyfrowanego pliku powinien być przekazany odbiorcy innym bezpiecznym kanałem (np. telefonicznie, przez SMS).

6.7. Technologicznie możliwe jest także wysyłanie wiadomości e-mail bez zabezpieczeń (tzw. otwartym tekstem). Z uwagi na związane z tym ryzyka dla poufności, a także dla integralności i dostępności przesyłanych informacji, nie jest rekomendowane przesyłanie wiadomości e-mail zawierających informacji poufne bez żadnych zabezpieczeń.

Przesyłanie informacji objętych tajemnicą zawodową lub danych osobowych za pośrednictwem poczty elektronicznej, w tym komunikacja z klientem

6.8. Wydaje się zasadnym, aby przy rozpoczęciu współpracy z klientem (przy przyjęciu zlecenia) poinformować klienta o zagrożeniach związanych z korzystaniem z poczty elektronicznej i prowadzeniem korespondencji między klientem a radcą prawnym za pomocą tego kanału komunikacji. W szczególności należy zwrócić uwagę na zagrożenia, które mogą wynikać dla klienta z ujawnienia korespondencji objętej tajemnicą zawodową (w tym o utracie poufności lub integralności takiej korespondencji). Radca prawny powinien też poinformować klienta, z jakich zabezpieczeń korzysta (np. że jego serwer pocztowy obsługuje szyfrowanie na poziomie transmisji za pomocą protokołu TLS). W takiej informacji można by 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).

6.9. 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.

6.10. Jednocześnie w takiej informacji dla klienta należy dodać, że jeżeli klient będzie korzystał z poczty elektronicznej do przekazywania radcy prawnemu informacji poufnych bez ustalania ewentualnych dodatkowych zabezpieczeń, to klient wyraża zgodę na stosowanie takiej formy komunikacji mimo potencjalnych związanych z tym ryzyk.

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

6.12. Ponadto, do wiadomości e-mail radca prawny powinien załączać krótką informację, że treść wiadomości jest poufna i chroniona tajemnicą zawodową i zastrzec, że jeżeli

osoba nie jest właściwym adresatem wiadomości, to powinna ona poinformować o tym jej nadawcę (radcę prawnego) i trwale tę wiadomość usunąć.

6.13. 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).

Uregulowanie rekomendacji w zasadach wewnątrzkorporacyjnych

6.14. Rekomendowane jest uregulowanie kwestii korzystania z poczty elektronicznej do przesyłania informacji objętych tajemnicą zawodową w wewnątrzkorporacyjnych aktach prawnych, np. w Regulaminie wykonywania zawodu radcy prawnego.

Pozostałe zasady dotyczące bezpieczeństwa informacji

6.15. Najczęściej występujące zagrożenia związane z korzystaniem z poczty elektronicznej to *phishing*, *malware* oraz *ransomware*. Należy jednak pamiętać, że istnieją także inne rodzaje zagrożeń dla ogólnie pojmowanego bezpieczeństwa informacji. Szerzej o poszczególnych zagrożeniach w pkt 5.3.-5.8 powyżej.

6.16. Przykładowe środki bezpieczeństwa, które powinien stosować radca prawny w związku z korzystaniem z poczty elektronicznej, są przedstawione poniżej. Poza tymi środkami należy także stosować środki w celu przeciwdziałania innym zagrożeniom bezpieczeństwa informatycznego, chociażby związane z bezpieczeństwem fizycznym sprzętu informatycznego lub bezpieczeństwem sieci.

- Należy każdorazowo weryfikować adres e-mail nadawcy, w tym sprawdzić, czy nadawca jest znany lub czy adres e-mail nadawcy zgadza się z dotychczas stosowanym adresem.
- Należy zwracać uwagę na treść wiadomości, zwłaszcza jeżeli otrzymana wiadomość pochodzi od nieznanego nadawcy. Należy zachować szczególną ostrożność klikając w linki lub otwierając załączniki zamieszczone w wiadomości.
- Należy zachować w poufności hasła do poczty elektronicznej i regularnie je zmieniać. Hasło nie powinno być oczywiste i łatwe do odgadnięcia przez osoby trzecie.
- Nie należy wykorzystywać służbowego adresu e-mail do wysyłania i odbierania wiadomości prywatnych.
- Nie należy przesyłać wiadomości służbowych na prywatne konto poczty elektronicznej.
- Należy pamiętać o bieżących aktualizacjach systemu operacyjnego oraz oprogramowania antywirusowego.
- Należy przeszkolić pracowników kancelarii w zakresie ochrony danych osobowych i podstawowych zasad bezpieczeństwa informacji oraz zobowiązać ich do stosowania się do powyższych zasad bezpieczeństwa.
- Zalecane jest wprowadzenie w kancelarii polityki korzystania z poczty elektronicznej.

6.17. Rekomendowane jest regularne sprawdzanie skuteczności i aktualizowanie środków bezpieczeństwa, które powinny obowiązywać zarówno radcę prawnego jak i innych pracowników i współpracowników kancelarii.

Opinia sporządzona w Kancelarii Traple, Konarski, Podrecki i Wspólnicy na zlecenie Ośrodka Badań, Studiów i Legislacji Krajowej Rady Radców Prawnych.

Opracowali:
dr Grzegorz Sibiga
Dominika Nowak
Katarzyna Syska
dr Iga Małobęcka-Szwast

Warszawa, 2020-06-08

Analiza porównawcza ogólnej zgodności chmurowych systemów pocztowych: Microsoft Exchange, Google GSuite

Porównanie wybranych systemów pocztowych wykonane zostało w celu udzielenia odpowiedzi czy korzystanie z tych aplikacji jest dopuszczalne zgodnie z przepisami o ochronie danych, w tym RODO[73], a także, czy wymienionych dostawców można wstępnie uznać za podmioty, które zapewniają wystarczające gwarancje stosowania przepisów o ochronie danych.

Analiza została wykonana w oparciu o materiały informacyjne i treści regulaminów/umów poszczególnych usług dostępne na stronach www dostawców tych rozwiązań (www.microsoft.com www.google.com) oraz na podstawie innych materiałów dostępnych w sieci.

Analiza dotyczy płatnych usług i pakietów dla przedsiębiorstw. Analiza nie dotyczy usług wskazanych dostawców w wersjach bezpłatnych.[74]

Usługi obu dostawców dostarczane są w ramach całego pakietu rozwiązań chmurowych i obejmują, wiele innych funkcjonalności oprócz samego serwera poczty elektronicznej.

Świadczenie usługi poczty elektronicznej polega na zapewnieniu specjalnego oprogramowania, tzw. „serwera pocztowego", umożliwiającego przesyłanie (wysyłanie i odbieranie) komunikatów do/od zdefiniowanych użytkowników. Każdy z użytkowników posiada określony(-e) adres(-y) pocztowy(-e) za pomocą którego (których) może wysyłać lub odbierać wiadomości. Serwer pocztowy jest oprogramowaniem, które dla swego działania musi być nieprzerwanie podłączony do sieci Internet.

Odczytywanie i nadawanie wiadomości przez użytkownika może odbywać się za pośrednictwem specjalnie przygotowanego interfejsu użytkownika, jak też za pośrednictwem zewnętrznego oprogramowania nazywanego „klientem pocztowym", instalowanego na urządzeniu użytkownika.

Dostawcy systemów pocztowych oferują obecnie również chmurowe wersje klientów pocztowych (serwisy webmail), które zapewniają możliwość odbierania i wysyłania wiadomości z adresów pocztowych różnych serwerów pocztowych. Przykładowo klient pocztowy www.outlook.live.com może obsługiwać adresy pocztowe z innych serwerów (np. darmowe @gmail.com lub adresy na serwerach organizacji), ale również klient pocztowy www.mail.google.com może obsługiwać pocztę z innych serwerów (np. darmowe @outlook.com lub adresy na serwerach organizacji).

Weryfikacja zgodności korzystania z usług poszczególnych dostawców z przepisami o ochronie danych powinna zatem dotyczyć oceny zgodności dostawcy w zakresie formalnych wymagań związanych z przetwarzaniem przez dostawcę danych osobowych, których administratorem pozostaje klient.

---

[73] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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) – zwane „**RODO**";

[74] Na uwagę zasługuje deklaracja Google w odniesieniu do usług reklamowych w usługach bezpłatnych GSuite: „*12.3 (..) ograniczenia odpowiedzialności mają zastosowanie w maksymalnym zakresie dopuszczalnym przez obowiązujące prawo, ale nie mają zastosowania w przypadku naruszania zobowiązań do zachowania poufności, naruszania przez jedną ze stron Praw własności intelektualnej drugiej strony ani w razie zobowiązań odszkodowawczych.",* zaś *„Informacje poufne" oznaczają informacje ujawniane przez jedną stronę drugiej stronie na mocy niniejszej Umowy, które zostały oznaczone jako poufne lub które zostałyby normalnie uznane za informacje poufne w danych okolicznościach. Dane klienta są Informacjami poufnymi Klienta.* Natomiast: *„Dane klienta" oznaczają dane (w tym pocztę e-mail) udostępniane, generowane, przekazywane lub wyświetlane za pośrednictwem Usług przez Klienta albo Użytkowników końcowych.* Wdaje się zatem, że Google potwierdza zachowanie poufności komunikacji (niewykorzystywanie danych dla własnych celów, w tym celów marketingowych) również w przypadku bezpłatnych usług GSuite.

W toku świadczenia usługi, w przypadku usług dla przedsiębiorstw, w ramach których poszczególne adresy/konta pocztowe tworzone oraz zarządzane są przez klienta, dostawca, co do zasady, będzie występował jako podmiot przetwarzający dane osobowe. Nie zmienia to faktu, że Google będzie uznany za administratora danych wobec danych telemetrycznych przetwarzanych w trakcie korzystania z usług Google lub generowanych automatycznie w wyniku korzystania z serwisów internetowych i przesyłanych do Google przez wydawców serwisów[75] lub w odniesieniu do danych pocztowych w sytuacji korzystania z bezpłatnych wersji dla użytkowników prywatnych.

Ocena kwestii formalnych:

Obaj badani dostawcy deklarują zgodność z przepisami o ochronie danych osobowych, w tym RODO, a weryfikacja dokumentów przedstawionych przez tych dostawców potwierdza ich twierdzenia. Każdy z dostawców oferuje inny sposób i zasady wykonania warunków umowy. Administrator danych pragnący skorzystać z usług któregoś z dostawców powinien szczegółowo przeanalizować poszczególne różnice zwracając uwagę na wpływ jaki wywołują one dla jego działalności.

Na uwagę zasługują w szczególności różnice związane z prawem umowy, sposobem realizacji obowiązku informowania o nowych podwykonawcach i skutkami złożenia sprzeciwu wobec takich dostawców oraz ogólnymi zasadami ograniczenia odpowiedzialności dostawcy.

Kryterium/obszar	Google GSuite	Microsoft Office 365
Strona umowy	Google LLC	Microsoft Ireland Operations Ltd.
Prawo umowy	USA, California	Irlandia[76]
Czy dane są przekazywane poza UE?	Dane telemetryczne połączenia użytkowników z usługą mogą być przekazywane poza UE.	Dane telemetryczne połączenia użytkowników z usługą mogą być przekazywane poza UE.
Obszar przetwarzania danych (Treści użytkowników)	Global/Region UE (możliwość ograniczenia obszaru przetwarzania do obszaru UE – usługi płatne)	Global/Region UE (możliwość ograniczenia obszaru przetwarzania do obszaru UE – usługi płatne)
Sposób informowania o podwykonawcach	Ogólna zgoda na podwykonawców Lista (dostępna w witrynie) Informacja 30 dni przed zaangażowaniem podmiotu	Ogólna zgoda na podwykonawców Lista (dostępna w witrynie) Informacja 14 dni przed zaangażowaniem podmiotu
Sprzeciw administratora	W przypadku sprzeciwu możliwość rozwiązania umowy.	W przypadku sprzeciwu możliwość rozwiązania umowy bez ponoszenia kar umownych
Czy jest DPA? (Umowa powierzenia zgodnie z art. 28 RODO)	Tak (należy aktywować umowę w portalu administracyjnym)	Tak
Czy DPA spełnia wymagania art. 28 RODO?	Tak	Tak
SCC (Standardowe klauzule umowne)	Tak (dołączone)	Tak (zawarte w DPA)

[75] Tutaj warto nadmienić, że zgodnie z ostatnimi wiadomościami, Google został pozwany USA za naruszenie prywatności użytkowników przeglądarki Chrome. Pozywający w pozwie zbiorowym domagają się 5 mld dolarów od Google'a. (https://biznes.wprost.pl/gospodarka/10331234/google-zaplaci-5-miliardow-dolarow-za-sledzenie-uzytkownikow-w-trybie-prywatnym.html)

[76] Brak jednoznacznego wskazania podmiotu świadczącego usługę. Zgodnie z deklaracją na stronie https://www.microsoft.com/pl-pl/servicesagreement/: Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521 Irlandia, Nr w rejestrze VAT IE8256796U.

Kryterium/obszar	Google GSuite	Microsoft Office 365
BCR (Wiążące reguły korporacyjne)	-	-
Privacy Shield	Tak	Tak
Ograniczenie odpowiedzialności	do 12 miesięcy dokonanych opłat (nie więcej niż 1000 USD dla usług bezpłatnych, jednak ograniczenie nie dotyczy naruszenia poufności, w tym Danych klienta)	do wpłaconej kwoty za usługi (do 5000 USD przy usługach bezpłatnych)

Ocena elementów bezpieczeństwa:

Obaj badani dostawcy deklarują stosowanie najwyższych środków bezpieczeństwa oraz ochronę poufności komunikacji. Ze względu na fakt iż serwis pocztowy jest jednym z szeregu usług świadczonych przez dostawców oraz że oferują oni również usługi bezpośrednio dotyczące bezpieczeństwa, ostateczna ocena zależeć będzie przede wszystkim od konfiguracji z której korzysta dana organizacja – klient dostawcy.

Obaj dostawcy gwarantują stosowanie środków oraz najnowszych standardów bezpieczeństwa w odniesieniu do przesyłanych wiadomości. Obaj dostawcy zapewniają również funkcje ochrony poczty przed działaniem oprogramowania złośliwego, ograniczanie podejrzanego ruchu i spamu, funkcje weryfikacji tożsamości wysyłającego dla poczty przychodzącej (w zakresie w jakim jest to możliwe, biorąc pod uwagę ograniczenia wynikające z charakterystyk wykorzystywanych powszechnie protokołów).

Badani dostawcy deklarują również zachowanie poufności danych w spoczynku (na kontach poszczególnych użytkowników) oraz szyfrowanie przesyłanych danych (szyfrowanie danych pomiędzy serwerami pocztowymi). Możliwe jest również uruchomienie pełnego szyfrowania treści wiadomości, jednakże z powodów organizacyjnych jest to funkcjonalność rzadko wykorzystywana w praktyce.[77]

Obaj dostawcy zapewniają także różnorodne środki stosowane celem ograniczenia dostępu do usługi dla osób nieupoważnionych, jak SSO, wieloskładnikowe uwierzytelnienie, czy też wsparcie dla oprogramowania zarządzającego hasłami - managerów haseł (Password managers). Dostawcy zapewniają również gamę alertów wspierających klienta w szybkim reagowaniu na pojawiające się zagrożenia lub awarie.

Podkreślenia wymaga, że właściwe uruchomienie poszczególnych funkcjonalności bezpieczeństwa oraz wybór sposobu uwierzytelnienia powinny zostać wykonane przez administratora usługi po stronie klienta.

[77] Stosowanie szyfrowania treści wiadomości w taki sposób, aby jedynie odbiorca mógł odczytać wiadomość wymaga uprzedniej wymiany kluczy służących do odszyfrowania wiadomości, pomiędzy wysyłającym a odbiorcą lub wprowadzenia innego sposobu jednoznacznej identyfikacji odbiorcy/nadawcy komunikatu. Serwery pocztowe muszą być jednak gotowe na sytuacje w których odbiorca co prawda nie jest zidentyfikowany lub nie będzie w posiadaniu klucza odszyfrowującego, ale nadawca decyduje jednak o chęci przesłania komunikatu. W praktyce większość korespondencji przesyłana jest w sposób jawny, a szyfrowana jest jedynie transmisja pomiędzy klientem a serwerem oraz pomiędzy serwerami pocztowymi. Jednocześnie użytkownik poczty może w danych okolicznościach samodzielnie skorzystać z szyfrowania E2EE.

Podsumowanie

Z analizy powyższych informacji (bazujących na deklaracjach dostawców usług) wynika, że, zasadniczo, wszyscy dostawcy deklarują stosowanie środków bezpieczeństwa na porównywalnym poziomie oraz zapewniają szeroką gamę środków do zastosowania według indywidualnych preferencji klienta.

Na podstawie powyższych ustaleń można potwierdzić zatem, że korzystanie z usług każdego z podmiotów objętych analizą będzie dopuszczalne zgodnie z RODO, a ostateczny wybór rozwiązania powinien być poprzedzony pogłębioną analizą technologiczną /bezpieczeństwa.

Koniecznością jest również korzystanie z wybranych narzędzi w sposób świadomy – zarówno przez użytkowników, organizatorów, jak również przez administratorów narzędzi po stronie organizacji.

Marcin Wielisiej
Data Processing Architects Sp. o. o.

Źródła i materiały:

Google

- Regulamin usługi bezpłatnej: https://gsuite.google.pl/intl/pl/terms/standard_terms.html
- Regulamin usług dla firm: https://gsuite.google.com/intl/pl/terms/2013/1/premier_terms.html
- Szczegółowe zasady świadczenia usług: https://gsuite.google.com/intl/en/terms/service-terms/
- Umowa powierzenia przetwarzania danych: https://gsuite.google.com/terms/dpa_terms.html
- Umowa powierzenia przetwarzania danych dla usług cloud: https://cloud.google.com/terms/data-processing-terms
- Standardowe klauzule umowne: https://gsuite.google.com/terms/mcc_terms.html
- Deklaracja dostosowania do RODO: https://www.google.com/cloud/security/gdpr/
- Deklaracja środków bezpieczeństwa infrastruktury Google: https://cloud.google.com/security/infrastructure/design/resources/google_infrastructure_whitepaper_fa.pdf
- Deklaracja szyfrowania danych w spoczynku: https://cloud.google.com/security/encryption-at-rest/default-encryption/resources/encryption-whitepaper.pdf
- Deklaracja szyfrowania danych w transmisji: https://cloud.google.com/security/encryption-in-transit/resources/encryption-in-transit-whitepaper.pdf
- Deklaracja środków bezpieczeństwa: https://services.google.com/fh/files/misc/google_security_wp.pdf

Microsoft

- https://www.microsoft.com/en-us/licensing/product-licensing/products
- https://www.microsoft.com/pl-pl/servicesagreement/
- Dokumentacja funkcjonalności Exchange dla różnych pakietów: https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-service-description?redirectedfrom=MSDN
- Opis funkcji bezpieczeństwa Exchange: https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-protection-service-description/exchange-online-protection-service-description

INNE:

- https://www.bralin.com/cloud-platform-security-showdown-g-suite-vs-office-365

Informacja dotycząca szyfrowania poczty elektronicznej przez wybranych dostawców

Kielce, 15 czerwca 2020 r.

Osoby przygotowujące informację

Damian Nartowski, radca prawny wpisany na listę radców prawnych prowadzoną przez Okręgową Izbę Radców Prawnych w Krakowie, nr wpisu: KR – 3733

Karol Wątrobiński, radca prawny wpisany na listę radców prawnych prowadzoną przez Okręgową Izbę Radców Prawnych w Krakowie, nr wpisu: KR – 3804. Zdobywca nagrody specjalnej w konkursie Rising Stars – Prawnicy Jutra.

Wątrobiński Nartowski sp. j., ul. Olszewskiego 6, 25-663 Kielce wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy w Kielcach, X Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000805378, NIP: 9592027315

Przedmiot informacji

1. Niniejsza informacja przedstawia kwestie szyfrowania poczty elektronicznej przez wybranych dostawców usług oraz wyniki weryfikacji dotyczącej tego, czy z usług tych dostawców mogą korzystać radcowie prawni w ramach swojej działalności zawodowej.

2. W informacji omówione zostaną usługi poczty elektronicznej świadczone przez:

   1) Google w ramach usługi Gmail, która jest częścią pakietu G Suite;

   2) Microsoft w ramach usługi Exchange Online, która jest samodzielną usługą, ale może być również częścią pakietu Microsoft 365 (dawniej Office 365);

   3) Apple w ramach usługi iCloud Mail, która jest częścią zestawu usług iCloud.

3. Informacja została sporządzona na podstawie regulaminów, warunków, polityk prywatności oraz innych dokumentów i materiałów dostępnych na stronach internetowych w/w dostawców oraz innych stronach internetowych.

4. Jeżeli było to możliwe, zamieściliśmy bezpośrednie linki odsyłające do stron internetowych, na których odnaleźliśmy powoływane dane lub informacje. W przypadku gdy były one ujęte w dokumentach lub materiałach, które można pobrać, podaliśmy link do takiego dokumentu lub materiału.

Wstęp

5. Kwestią niepodlegającą dyskusji w środowisku radców prawnych jest to, że fizyczne wersje dokumentów (np. wydruki) muszą być zabezpieczone w odpowiedni sposób. Odpowiedni, czyli taki, który uniemożliwi dostęp do dokumentów osobom do tego niepowołanym (choćby przez przypadek). Nawet jeśli niekiedy praktyka przechowywania fizycznych dokumentów nieco odbiega od oczekiwanych standardów, to świadomość, że muszą one być dobrze chronione jest powszechna.

6. Wydaje się, że nieco inaczej wygląda sytuacja w przypadku cyfrowych wersji dokumentów. Praktyka pokazuje, że poziom świadomości dotyczący ustalenia zagrożeń jakie potencjalnie mogą być związane z przechowywaniem dokumentów w chmurze czy przesyłaniem ich e-mailem jest niższy niż w przypadku identyfikowania zagrożeń dotyczących nośników fizycznych. Wynika to oczywiście z tego, że ustalenie cyfrowych zagrożeń wymaga posiadania pewnej wiedzy „technicznej" i nie jest tak intuicyjne.

7. Niewątpliwie już wcześniej poczta elektroniczna była dla zdecydowanej większości radców prawnych zupełnie podstawowym narzędziem pracy i głównym kanałem komunikacji z klientami. Ostatnie miesiące pokazały jednak, że w zasadzie jest to narzędzie bez którego obecnie nie można się już obejść.

8. Trzeba też pamiętać, że informatyzacja postępowań sądowych (choć postępuje bardzo powoli) prawdopodobnie spowoduje kolejny wzrost znaczenia tego środka komunikacji w działalności radców prawnych.

9. Już teraz, w aktualnym stanie prawnym, w sprawach gospodarczych wskazanie adresu poczty elektronicznej lub złożenie oświadczenia, że takiego adresu się nie posiada jest konieczne do tego, by sprawie został nadany bieg (pozew, art. 458(3) § 1 k.p.c.) albo żeby pozwany skutecznie wniósł pierwsze pismo w sprawie (np. odpowiedź na pozew, sprzeciw, zarzuty; art. 458(3) § 2 k.p.c.). Zaniechanie realizacji tego obowiązku stanowi brak formalny.

10. Co więcej, wskazanie adresu poczty elektronicznej może ułatwić komunikację, w tym umożliwić przeprowadzenie rozprawy w sposób zdalny. Przykładowo w ostatnim czasie otrzymaliśmy wezwanie do wskazania adresu poczty elektronicznej w celu przesłania na ten adres linku, który umożliwi przeprowadzenie rozprawy, pod rygorem uznania, że adresu poczty elektronicznej pełnomocnik nie posiada.

11. Złożenie przez pełnomocników stron zgodnych oświadczeń, co do dokonywania wzajemnych doręczeń za pośrednictwem poczty elektronicznej i wskazanie adresów e-mail powoduje, że pełnomocnicy są związani tym sposobem wymiany korespondencji pomiędzy sobą przy

składaniu pism procesowych niewymienionych w art. 132 § 1(1) k.p.c., chyba że sąd zarządzi odstąpienie od takiej formy prowadzenia korespondencji (art. 132 § 3(1) k.p.c.).

12. W naszej ocenie radcowie prawni powinni z dużą uwagą podchodzić do wyboru narzędzi, które umożliwiają im elektroniczne komunikowanie się z klientami. W szczególności zaś do wyboru dostawcy poczty elektronicznej, skoro dla większości z nich jest to jedno z najważniejszych narzędzi pracy.

13. Radcowie prawni muszą w tym zakresie zwrócić uwagę na obowiązki wynikające z przepisów ustawy o radcach prawnych, Kodeksu Etyki Radcy Prawnego, Regulaminu wykonywania zawodu radcy prawnego oraz RODO.

14. Odpowiedni wybór dostawcy poczty elektronicznej wiąże się z przestrzeganiem tajemnicy zawodowej (art. 23 KERP, § 6 ust. 1 Regulaminu) oraz zapewnieniem bezpieczeństwa danych osobowych (art. 5 ust. 1 lit. f) RODO), które niewątpliwie radca prawny przetwarza wykonując zawód.

15. Wykonywanie drogą elektroniczną czynności zawodowych przez radcę prawnego wymaga spełnienia warunków określonych w art. 35 KERP. Przepis ten został umieszczony w rozdziale zatytułowanym “Informowanie o wykonywaniu zawodu oraz pozyskiwanie klientów”. Jednak w istocie jest to przepis ogólny, który wskazuje jakie warunki musi spełnić radca prawny by w ogóle móc skorzystać ze środków komunikacji elektronicznej przy realizacji czynności zawodowych.

16. Niezależnie od podstawowych wymogów narzucanych w art. 35 pkt. 1 oraz 2 KERP dotyczących tego w jaki sposób stworzyć adres poczty elektronicznej, to wymienione zostały w art. 35 KERP obowiązki związane z koniecznością prowadzenia okresowej archiwizacji przetwarzanych drogą elektroniczną danych w celu ich zabezpieczenia i ochrony dostępności (art. 35 pkt. 6 KERP) czy ochrony tajemnicy zawodowej (art. 35 pkt 7 KERP).

17. W odniesieniu do ostatniego, ale niezwykle istotnego punktu art. 35 KERP należy zwrócić uwagę, że nie tylko nakłada on obowiązek informowania w treści korespondencji elektronicznej o jej poufnym charakterze. Artykuł 35 pkt 7 KERP wskazuje też – dość przewrotnie – jakie zabezpieczenie należy uznać za odpowiednie: jeżeli klient po uprzednim poinformowaniu go o zagrożeniach związanych z korzystaniem z drogi elektronicznej, domyślnie lub wyraźnie zaakceptował stosowane w komunikacji z nim środki, techniki, sposoby, systemy lub standardy komunikacji elektroniczne to uznaje się wykorzystywane zabezpieczenie za adekwatne (należyte).

18. Postanowienia RODO również nakładają na radcę prawnego obowiązek wdrożenia odpowiednich środków technicznych lub organizacyjnych, które zapewnią odpowiednie bezpieczeństwo danych osobowych przetwarzanych przez radcę prawnego, w tym ochronę przed niedozwolonym lub

niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem (art. 5 ust. 1 lit. f) RODO).

19. Regulacje korporacyjne są szersze zakresowo niż postanowienia RODO, bowiem odnoszą się również do materiałów, które nie zawierają danych osobowych, ale stanowią nośnik informacji objętych tajemnicą zawodową. Nie przeszkadza to jednak w wykorzystywaniu procedur i standardów wprowadzanych w związku z wdrożeniem przepisów RODO do dostosowania funkcjonowania Kancelarii w zgodzie z oboma tymi reżimami prawnymi.

Wybór dostawcy poczty elektronicznej

20. Truizmem byłoby stwierdzenie, że przed rozpoczęciem korzystania z usług konkretnego dostawcy poczty elektronicznej przede wszystkim należy zweryfikować warunki dotyczące świadczenia takich usług. Jak jednak pokazuje praktyka, zdarza się, że radca prawny wybiera narzędzie, które nie do końca nadaje się do wykorzystywania go przy świadczeniu usług prawnych.

21. Przykładowo, w warunkach świadczenia usług, które podaje jeden z popularnych dostawców darmowej poczty elektronicznej, wskazano wprost, że ma on prawo do używania automatycznych systemów i algorytmów do analizowania treści użytkownika. Potencjalnie oznacza to, że system może analizować treść e-maili przesyłanych i otrzymywanych przez radcę prawnego.[78] Takie postanowienie – choć nie zakłada, że dostęp do treści wiadomości będą mieli ludzie, musi budzić pewien niepokój w kontekście zasad etyki.[79] Dostawca ten udostępnia jednak płatną wersję usługi, w której takiego postanowienia już nie ma.

22. Choć nie jest to poparte żadnymi badaniami, a jedynie naszymi obserwacjami, to mamy wrażenie, że przypadki korzystania przez radców prawnych z darmowej poczty elektronicznej nie są jednostkowe. Co prawda nie można z góry założyć, że używanie darmowych skrzynek mailowych przez radców prawnych jest niedozwolone. Jednak radca prawny, który chce korzystać z takiej usługi musi szczególnie uważnie zapoznać się z warunkami jej świadczenia. W przypadku niektórych darmowych usług, dostawcy wprost zastrzegają, że nie można ich wykorzystywać do komercyjnej działalności. Znaczenie ma więc nie tyle kwestia odpłatności usługi, co konkretne postanowienia regulaminów.

---

[78] Zob. również S. Wikariak, *Treść wysyłanej poczty jest skanowana. Prawnicy nie powinni korzystać z darmowych kont*, Dziennik Gazeta Prawna, 23 stycznia 2020 r., https://prawo.gazetaprawna.pl/artykuly/1449979,poczta-gmail-skanowanie-tresci-wiadomosci-prawnik.html, dostęp na dzień 14 czerwca 2020 r.

[79] Por. jednak opinię nr 820 New York State Bar Association z dnia 2 sierpnia 2018 r., w której wskazano, że tamtejsi prawnicy mogą korzystać z usług dostawców poczty elektronicznej, który przeprowadza komputerowe skanowanie e-maili w celu targetowania reklam, jeśli e-maile nie są przeglądane przez ludzi, https://nysba.org/ethics-opinion-820/, dostęp na dzień 14 czerwca 2020 r.

23. Po wstępnym zweryfikowaniu, czy usługa w ogóle nadaje się do biznesowego użycia, należy zwrócić uwagę na kwestię bezpieczeństwa gwarantowanego przez usługodawcę.

24. Jednym z głównych ryzyk korzystania z e-maili jest to, że z przechowywanymi lub przesyłanymi wiadomościami zapozna się nieuprawniona osoba. Stąd pojawia się pytanie o potrzebę szyfrowania poczty elektronicznej. Jest ono jednym z podstawowych sposobów zapewnienia poufności przesyłanych informacji.

25. Z góry wskazujemy, że w analizie skupimy się na szyfrowaniu zapewnianym bezpośrednio przez dostawców poczty. Nie będziemy zajmować się szczegółowo możliwością dodatkowego konfigurowania klientów poczty elektronicznej, na przykład przez korzystanie z systemu PGP umożliwiającego szyfrowanie treści wiadomości. W przypadku korzystania z takiego szyfrowania wybór usługi ma bowiem mniejsze znaczenie. Wspomnimy jednak o takiej opcji, tam gdzie usługodawcy informują o możliwości skorzystania z dodatkowego szyfrowania.

26. Wskazujemy również na rozróżnienie, które trzeba poczynić pomiędzy wspomnianymi przed chwilą klientami poczty elektronicznej a usługą (hostingiem) poczty.

27. Klientem poczty elektronicznej jest program służący do wysyłania i odbierania wiadomości e-mail – na przykład Outlook lub Thunderbird. W programie tym można dodać konto pocztowe, które jest obsługiwane przez zupełnie innego dostawcę. Przykładowo w programie Outlook (dostarczanym przez Microsoft) można skonfigurować konto Gmail (dostarczane przez Google). Dla niniejszej informacji istotne jest, kto dostarcza pocztę i jakie szyfrowanie zapewnia. W klientach poczty elektronicznej można samodzielnie skonfigurować dodatkowe narzędzia do szyfrowania, o czym przed chwilą wspomnieliśmy.

Szyfrowanie

28. Jak się wskazuje: „Szyfrowanie jest głównym zastosowaniem kryptografii: sprawia, że dane stają się niezrozumiałe, co ma zapewnić ich poufność. W szyfrowaniu stosowany jest algorytm nazywany szyfrem oraz sekretna wartość nazywana kluczem. Jeśli nie znamy klucza, nie możemy odszyfrować ani nawet poznać kawałka informacji z zaszyfrowanego komunikatu – nie może też tego zrobić żaden napastnik.”[80]

29. Wspomniane wyżej szyfrowanie poczty elektronicznej oznacza (w dużym uproszczeniu) takie zabezpieczenie treści wiadomości lub połączenia, że w przypadku przechwycenia tej wiadomości, jest ona nieczytelna dla osób, które nie posiadają klucza umożliwiającego jej odszyfrowanie. Zatem

[80] Jean-Philippe Aumasson, *Nowoczesna kryptografia,* Wydawnictwo Naukowe PWN, 2018, str. 24.

nawet jej przechwycenie przez osobę nieuprawnioną nie spowoduje, że będzie ona mogła być przez taką osobę odczytana.

30. Na potrzeby tej informacji możemy wyróżnić kilka rodzajów zastosowań szyfrowania.

31. Po pierwsze, dane mogą być szyfrowane podczas ich przechowywania. W takim przypadku mówimy o szyfrowaniu „w spoczynku" („at-rest encryption"). W szyfrowaniu danych „w spoczynku" chodzi o zabezpieczenie danych, które są przechowywane na serwerach dostawcy. W przypadku poczty elektronicznej szyfrowane mogą być więc maile oraz załączniki przechowywane na takich serwerach. Ma to chronić te dane przed dostępem nieuprawnionych osób z zewnątrz.

32. Szyfrowanie danych „w spoczynku" nie oznacza jednak w większości przypadków, że nie ma do nich dostępu usługodawca. Zwykle to on dysponuje odpowiednim kluczem umożliwiającym odszyfrowanie, więc mógłby zapoznać się z danymi. Pełne szyfrowanie tzn. takie, które nawet dostawcy uniemożliwia wgląd do treści danych (tzw. „zero-knowledge encryption") potencjalnie jest możliwe, jednak (jak się okaże) nie w przypadku standardowych usług poczty elektronicznej.

33. Po drugie, dane mogą być szyfrowane „w trakcie przesyłu" („in transit encryption"). W tym przypadku chodzi z kolei o zabezpieczenie danych w trakcie kiedy są przesyłane z jednej maszyny do innej (np. od nadawcy e-maila do jego odbiorcy).

34. Protokołem służącym do takiej ochrony jest Transport Layer Security (TLS). Protokół ten dawniej był znany jako SSL. Przez lata publikowano kolejne wersje protokołu TLS – od wersji 1.0 do 1.3. Protokół ten zabezpiecza połączenie między użytkownikiem serwerami.[81] TLS szyfruje połączenie, a nie bezpośrednio treść wiadomości.

35. Jak się wskazuje „jednym z celów bezpieczeństwa TLS jest zapobieganie atakom typu man, gdzie napastnik przejmuje zaszyfrowany ruch od strony nadającej, odszyfrowuje go, aby uzyskać jawną zawartość, a następnie ponownie szyfruje, aby wysłać do odbiorcy. TLS pokonuje ataki man-in-the-middle za pomocą uwierzytelnionych serwerów (i opcjonalnie klientów) oraz certyfikatów i zaufanych centrów certyfikacji […]."[82]

36. Przy szyfrowaniu „w trakcie przesyłu" trzeba jednak pamiętać, że faktyczne stosowanie tego szyfrowania zależy nie tylko od nadawcy, ale również od odbiorcy. Jeśli bowiem ustawienia serwera, z którego korzysta nadawca wspierają protokół TLS, ale serwer odbiorcy nie używa tego protokołu, to szyfrowanie nie będzie w pełni skuteczne. Szyfrowanie nastąpi w trakcie połączenia

[81] Na temat szczegółów działania tego protokołu zobacz więcej: M. Karbowski, *Podstawy kryptografii. Wydanie III*, Helion, 2015, str. 154 i nast.
[82] Jean-Philippe Aumasson, *Nowoczesna kryptografia,* Wydawnictwo Naukowe PWN, 2018, str. 353.

z serwerem pocztowym nadawcy, ale od momentu przekazania wiadomości między serwerem nadawcy a serwerem odbiorcy wiadomość szyfrowana nie będzie.

37. Po trzecie, możliwe jest stosowanie dodatkowego szyfrowania, w przypadku którego treść wiadomości podlega zaszyfrowaniu przez nadawcę i pozostaje zaszyfrowana przez czas jej transmitowania do odbiorcy. Tylko odbiorca dysponujący odpowiednim kluczem może ją odszyfrować (tzw. szyfrowanie „end to end").

38. Bardzo popularnym systemem umożliwiającym to szyfrowanie jest PGP (Pretty Good Privacy), który działa w oparciu o klucze prywatne i publiczne. Aby możliwe było skorzystanie z tego oprogramowania musi je zainstalować zarówno nadawca jak i odbiorca wiadomości. Powoduje to, że korzystanie z tego rozwiązania jest nieco bardziej skomplikowane.[83]

39. Drugim popularnym systemem umożliwiającym dodatkowe szyfrowanie jest S/MIME (Secure/Multipurpose Internet Mail Extension). Również w tym przypadku konieczne jest by z tego systemu korzystał zarówno nadawca jak i odbiorca. Użytkownicy muszą się więc wymienić kluczami, po to aby mogli odszyfrowywać swoje wiadomości. Także w tym przypadku jest więc potrzebne podjęcie dodatkowych działań przez obie strony, które się komunikują.

40. Niezależnie od kwestii szyfrowania połączeń czy treści wiadomości, warto również zwrócić uwagę na możliwość zabezpieczenia załączników do e-maila.

41. Załącznik taki (np. dokument Microsoft Word) w bardzo prosty sposób można zabezpieczyć hasłem. Nawet w przypadku przejęcia e-maila przez osobę nieuprawnioną (co może nastąpić chociażby przez wysyłkę do błędnego adresata) załącznik taki nie zostanie otwarty, ponieważ osoba nieuprawniona nie będzie znała hasła. Hasło takie powinno zostać przesłane odbiorcy innym kanałem komunikacji (np. wiadomością SMS). Przesyłanie hasła mailem (w skrajnych przypadkach tym samym, którym przesyłany jest załącznik) nie ma oczywiście żadnego sensu i nie poprawia bezpieczeństwa.

G suite (gmail)

42. Usługa Gmail dostarczana przez Google pozostaje jedną z najbardziej popularnych skrzynek mailowych, z której korzystają polscy internauci. Darmowa wersja tej usługi nie jest odpowiednia (w naszej ocenie) do stosowania przez radców prawnych. Google udostępnia jednak płatną wersję

[83] Na pewne trudności związane ze stosowaniem takiego rozwiązania zwrócił również uwagę ówczesny Generalny Inspektor Ochrony Danych Osobowych; zob. *Opinia w sprawie bezpieczeństwa danych przekazywanych przy użyciu poczty elektronicznej*, str. 3.

tej usługi, którą radcowie prawni mogą rozważyć jako opcję do korzystania. Płatna wersja tej usługi jest dostępna w ramach pakietu G Suite i to ona zostanie poniżej omówiona.

43. Google publikuje na swoich stronach internetowych wiele informacji na temat zasad, w oparciu o które szyfruje dane użytkowników G Suite.

44. Przede wszystkim Google wskazuje, że w przypadku Gmaila szyfrowane są zarówno wiadomości, jak i załączniki.[84]

45. Szyfrowanie danych odbywa się w sposób automatyczny tzn. użytkownik nie musi wykonywać żadnych działań w celu jego uruchomienia.

46. Szyfrowanie obejmuje zarówno dane „w spoczynku" jak i „w trakcie przesyłu".

47. Jeśli chodzi o szyfrowanie danych „w spoczynku" to odbywa się ono w momencie zapisu na dysku i obejmuje również kopie zapasowe danych.

48. Klucz szyfrowania jest powiązany z tzw. Access Control List (ACL). Według Google stosowanie ACL zapewnia gwarancję, że dane mogą być odszyfrowane tylko przez osoby, które Google do tego upoważniło.[85] To jednak potwierdza, że nie mamy tu do czynienia z „zero-knowledge encryption".

49. Zasady dostępu do danych użytkownika opisano szerzej w dokumencie „Google Cloud whitepapper Trusting your data with G Suite").[86] Zgodnie z informacjami, które się w nim znajdują, Google nie będzie korzystać z danych użytkowników w celach innych niż te, które są niezbędne do wypełnienia zobowiązań umownych Google. Google deklaruje, że ogranicza liczbę pracowników mających dostęp do danych użytkowników i aktywnie monitoruje aktywność tych pracowników.

50. Google oświadcza, że używa różnych kluczy, nawet jeśli dane należą do tego samego klienta. Dane są szyfrowane przy użyciu 128-bitowego (lub silniejszego) algorytmu Advanced Encryption Standard (AES).[87]

---

[84] „G Suite Encryption Whitepaper", https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf, str. 4, dostęp na dzień 14 czerwca 2020 r.; w dokumencie tym brak niestety jest daty jego sporządzenia, jednak do powoływanej w tej informacji wersji dokumentu odwołują się inne dokumenty opracowane przez Google, w tym dokument „Google Cloud whitepaper" z grudnia 2019 r., stąd też uznajemy dokument „G Suite Encryption Whitepaper" w powoływanej tutaj wersji za aktualny.

[85] „G Suite Encryption Whitepaper", https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf, str. 3, dostęp na dzień 14 czerwca 2020 r.

[86] Google Cloud whitepapper", https://cloud.google.com/files/gsuite-trust-whitepaper.pdf, grudzień 2019, str. 10-11, dostęp na dzień 14 czerwca 2020 r.

[87] „G Suite Encryption Whitepaper", https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf, str. 3, dostęp na dzień 14 czerwca 2020 r.

51. E-maile w przypadku korzystania z usługi G Suite są również szyfrowane „w trakcie przesyłu” – to znaczy w momencie ich przesyłania od użytkownika na serwery Google oraz między centrami danych Google.

52. W tym przypadku szyfrowanie również następuje automatycznie i obejmuje ruch między urządzeniem użytkownika a serwerami Google. Według Google szyfrowanie danych odbywa się na kilku poziomach.

53. Po pierwsze Google stosuje protokół HTTPS dla połączeń pomiędzy użytkownikiem usług wchodzących w skład G Suite (w tym Gmaila). Dodatkowo Google szyfruje transmisję wiadomości z innymi serwerami pocztowymi przez używanie 256-bitowego TLS.[88]

54. Protokół TLS jest dostępny dla wszystkich użytkowników G Suite – niezależnie od konkretnego abonamentu, z którego użytkownik korzysta (Basic, Business, czy Enterprise). G Suite obsługuje TLS w wersjach 1.0, 1.1, 1.2 i 1.3.

55. Jak jednak już wspomniano faktyczna skuteczność szyfrowania z użyciem TLS zależy od tego, czy z tego protokołu korzystają obie strony komunikacji. Google wprost o tym informuje:[89]

> Aby utworzyć bezpieczne połączenie, zarówno nadawca, jak i adresat muszą używać protokołu TLS. Gdy bezpieczne połączenie nie jest dostępne, Gmail dostarcza wiadomości przez połączenia niezabezpieczone.

56. Co jednak ciekawe, istnieje opcja „zmuszenia” do stosowania TLS. Według informacji przekazywanych przez Google:[90]

> Możesz jednak skonfigurować ustawienie TLS w taki sposób, aby bezpieczne połączenie było wymagane w przypadku wymiany e-maili z określonymi domenami lub adresami e-mail.
>
> **Ważne:** zalecamy skonfigurować ustawienie TLS w taki sposób, by usługa Gmail *zawsze* korzystała z bezpiecznych połączeń w przypadku wysyłania i odbierania e-maili z konkretnych domen i adresów e-mail.

57. Oznacza to więc, że potencjalnie można „wymusić” bezpieczne połącznie w przypadku komunikacji np. z konkretnym klientem. Jeśli w przypadku tego klienta okaże się, że TLS nie jest dostępny, to e-mail od radcy prawnego nie zostanie wysłany.

---

[88] Szczegóły na temat mechanizmów szyfrowania połączeń TLS w Gmailu dostępne są pod tym linkiem: https://support.google.com/a/answer/9795993?hl=pl&ref_topic=2683824, dostęp na dzień 14 czerwca 2020 r.

[89] https://support.google.com/a/answer/2520500?hl=pl&ref_topic=2683824, dostęp na dzień 14 czerwca 2020 r.

[90] https://support.google.com/a/answer/2520500?hl=pl&ref_topic=2683824, dostęp na dzień 14 czerwca 2020 r.

58. Warto zapoznać się z „Raportem Przejrzystości", w ramach którego Google publikuje informacje na temat tego, jaki procent e-maili przesyłanych lub otrzymywanych przez użytkowników Gmaila jest szyfrowany. Według najnowszych informacji zarówno szyfrowanie wiadomości wychodzących z Gmaila do użytkowników innych domen, jak i wiadomości przychodzących do Gmaila od użytkowników innych domen kształtuje się na poziomie 94%.[91]

59. Dodatkowo trzeba odnotować, że w przypadku abonamentu G Suite Enterprise, Google stosuje rozszerzony standard szyfrowania S/MIME. S/MIME ma na celu szyfrowanie wiadomości na drodze od nadawcy do odbiorcy. Aby używać tego rozwiązania, nadawca i adresat muszą mieć aplikację poczty obsługującą ten standard.

60. W przypadku korzystania z Gmaila przez przeglądarkę internetową lub aplikację mobilną można łatwo sprawdzić poziom szyfrowania wysyłanych i otrzymywanych wiadomości przez weryfikację ikony widocznej przy wiadomości:[92]

- **Zielony (ulepszone szyfrowanie S/MIME)** – poziom odpowiedni do przesyłania większości poufnych informacji. Protokół S/MIME szyfruje wszystkie wiadomości wychodzące, jeśli mamy klucz publiczny odbiorcy. Tylko odbiorca mający odpowiedni klucz prywatny może odszyfrować e-maila.
- **Szary (standardowe szyfrowanie TLS)** – poziom odpowiedni do przesyłania większości wiadomości. Protokół TLS (Transport Layer Security) jest używany podczas wymiany e-maili z innymi usługami pocztowymi, które nie obsługują S/MIME.
  Wskazówka: obsługa TLS nie jest gwarantowana i zależy od wcześniejszej komunikacji z usługą poczty e-mail odbiorcy.
- **Czerwony (bez szyfrowania)** – niezaszyfrowana poczta, która nie jest bezpieczna. Do określania, czy wysyłana wiadomość zostanie wiarygodnie zaszyfrowana, używane są e-maile, które zostały wcześniej wysłane do domeny adresata.

Microsoft 365 (Exchange Online)

61. Aplikacje do pracy biurowej dostarczane przez Microsoft są od lat podstawowym narzędziem pracy dla radców prawnych. W ramach płatnej platformy Microsoft 365 (dawniej Office 365) można korzystać m.in. z usługi Exchange Online. Usług ta jest dostępna również poza platformą Microsoft 365 – bez konieczności kupowania aplikacji pakietu Office.

62. Jedną z aplikacji wspomnianego pakietu Office jest program Outlook, który jest klientem poczty elektronicznej. Jak już wyżej wspomnieliśmy, w takim programie można skonfigurować konto pocztowe, które jest obsługiwane przez innego usługodawcę. Na potrzeby tej informacji nie będziemy jednak analizować działania programu Outlook, a jedynie kwestie związane z pocztą

[91] https://transparencyreport.google.com/safer-email/overview?email_domain_results=q:allegro.pl&email_domain_search=encryption_level:RED,YELLOW;q:allegro.pl&lu=email_domain_results, dostęp na dzień 14 czerwca 2020 r.
[92] https://support.google.com/mail/answer/6330403?hl=pl, dostęp na dzień 14 czerwca 2020 r.

elektroniczną dostarczaną przez Microsoft. Usługa Exchange Online może być oczywiście połączona z programem Outlook.

63. Podobnie jak Google, Microsoft publikuje na swoich stronach internetowych liczne materiały, w których opisuje stosowane standardy szyfrowania. Część z tych informacji pochodzi sprzed zmiany nazwy z Office 365 na Microsoft 365, jednak zakładamy, że używane zabezpieczenia się nie zmieniły, a dostępne informacje pozostają aktualne.

64. Microsoft informuje, że dane użytkowników są szyfrowane zarówno „w spoczynku" jak i „w trakcie przesyłu".[93] Zasadniczo szyfrowanie jest domyślne i nie wymaga od użytkownika wprowadzania zmian w konfiguracji.[94] Użytkownicy mają jednak możliwość wyboru dodatkowych opcji, o czym będzie jeszcze mowa.

65. Microsoft deklaruje, że szyfrowanie „w spoczynku" obejmuje zarówno wiadomości e-mail, jak i załączniki. Microsoft wykorzystuje w swoich centrach danych BitLocker, czyli rozwiązanie pozwalające na szyfrowanie przy pomocy algorytmu AES (128-bitowego lub 256-bitowego). Rozwiązanie to może być zresztą wykorzystywane również na komputerach użytkowników, którzy korzystają z systemu Windows.[95]

66. Microsoft deklaruje również, że w swoich centrach danych używa tzw. technologii „Distributed Key Manager" (DKM). Dotyczy to również danych w Exchange Online. DKM jest funkcją pozwalającą na używanie zestawu tajnych kluczy do szyfrowania i odszyfrowania informacji. W przypadku usługi Exchange Online dostęp do tych kluczy będzie możliwy wyłącznie z poziomu niektórych kont. Według informacji przekazywanych przez Microsoft w przypadku ich centrów danych, żadne osoby (w ramach standardowych procedur), nie otrzymują dostępu do kluczy, które mogą odszyfrować te informacje. Dostęp taki może zostać udzielony w przypadku gdy będzie to potrzebne np. w celu rozwiązania problemów, ale wymaga zatwierdzenia.[96]

67. Szyfrowanie danych „w trakcie przesyłu" może nastąpić gdy:

1) urządzenie użytkownika komunikuje się z serwerami Microsoft;

2) serwer Microsoft komunikuje się z innym serwerem Microsoft;

---

93 https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption?view=o365-worldwide, dostęp na dzień 14 czerwca 2020 r.

94 https://docs.microsoft.com/en-us/microsoft-365/compliance/email-encryption?view=o365-worldwide, dostęp na dzień 14 czerwca 2020 r.

95 Zob. więcej https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview, dostęp na dzień 14 czerwca 2020 r.

96 https://docs.microsoft.com/en-us/microsoft-365/compliance/exchange-online-secures-email-secrets?view=o365-worldwide, dostęp na dzień 14 czerwca 2020 r.

3) serwer Microsoft komunikuje się z serwerem innego podmiotu niż Microsoft.[97]

68. W przypadku korzystania z usługi Exchange Online serwery Microsoftu zawsze szyfrują połączenie z innymi serwerami Exchange Online z użyciem TLS w wersji 1.2.[98] W informacji datowanej na 2019 r. Microsoft wskazuje, że pakiet Office 365 nie wspiera TLS w wersji 1.3.[99]

69. TLS wykorzystywany jest domyślnie. Jak już jednak wspomniano faktyczna skuteczność takiego szyfrowania zależy oczywiście od tego, czy z TLS korzysta również odbiorca wiadomości. Według Microsoft, usługa Exchange Online może zostać skonfigurowana tak by wiadomości do konkretnego odbiorcy zawsze były wysyłane z użyciem bezpiecznego połączenia. Podobnie jak w przypadku Gmaila, można więc „wymusić" stosowanie TLS. Jeśli taka opcja nie została wybrana, a odbiorca nie obsługuje TLS, to wiadomość zostanie wysłana bez szyfrowania.[100]

70. Microsoft udostępnia dodatkowe opcje umożliwiające szyfrowanie poczty elektronicznej. Takimi dodatkowymi opcjami są m.in.:

1) Secure/Multipurpose Internet Mail Extensions (S/MIME);

2) Office Message Encryption (OME);

71. Jak już wspomnieliśmy, S/MIME to rozszerzony standard szyfrowania mający na celu zaszyfrowanie wiadomości na drodze od nadawcy do odbiorcy. Korzystanie z protokołu S/MIME jest możliwe w przypadku gdy użytkownik korzysta z Outlooka w wersji 2010 lub nowszej, Outlooka w wersji webowej (przez przeglądarkę) lub z Exchange ActiveSync.[101]

72. OME jest z kolei usługą Microsoft, która pozwala przesyłać zaszyfrowane wiadomości e-mail bez względu na to do jakiego adresata są przesyłane. Użytkownik może ustawić aby szyfrowanie działało automatycznie. Odbiorca zaszyfrowanej wiadomości, aby móc się z nią zapoznać musi wygenerować jednorazowe hasło lub na przykład zalogować się na konto Microsoft. Klucze są przechowywane przez Microsoft. Istnieje możliwość wprowadzenia ustawień zgodnie z którymi

97 https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-for-data-in-transit?view=o365-worldwide, dostęp na dzień 14 czerwca 2020 r.

98 https://docs.microsoft.com/en-us/microsoft-365/compliance/exchange-online-uses-tls-to-secure-email-connections?view=o365-worldwide, dostęp na dzień 14 czerwca 2020 r.

99 https://docs.microsoft.com/en-us/microsoft-365/compliance/technical-reference-details-about-encryption?view=o365-worldwide, dostęp na dzień 14 czerwca 2020 r.

100 https://docs.microsoft.com/en-us/microsoft-365/compliance/exchange-online-uses-tls-to-secure-email-connections?view=o365-worldwide, dostęp na dzień 14 czerwca 2020 r.

101 Zob. więcej https://docs.microsoft.com/en-us/Exchange/policy-and-compliance/smime/smime?view=exchserver-2019, dostęp na dzień 14 czerwca 2020 r.

szyfrowane będą wszystkie wiadomości adresowane do konkretnej osoby (np. konkretnego klienta radcy prawnego) lub wszystkie wiadomości, które zawierają konkretne słowo w temacie.[102]

73. Wydaje się, że OME w praktyce może być interesującą i relatywnie prostą opcja szyfrowania najważniejszych wiadomości. Co ciekawe, Microsoft wprost wskazuje, że w ich ocenie może być odpowiednia do używania przez prawników: „We recommend using OME when you want to send sensitive business information to people outside your organization, whether they're consumers or other businesses. For example: […] An attorney sending confidential legal information to another attorney". Wiadomości zaszyfrowane dzięki tej funkcji mogą być wysyłane także do osób korzystających z poczty elektronicznej innych podmiotów (np. z Gmaila).[103]

74. Funkcja ta nie jest jednak obecnie dostępna we wszystkich pakietach Microsoft 365, dlatego trzeba zweryfikować czy wybrany pakiet Microsoft 365 pozwala na skorzystanie z niej.

iCloud

75. Jednym z dostawców poczty elektronicznej jest również Apple. Z tej poczty można korzystać w ramach zestawu usług iCloud, który jest przeznaczony dla użytkowników urządzeń Apple. Usługa iCloud w podstawowej wersji jest bezpłatna. Użytkownik ponosi koszty w przypadku gdyby chciał korzystać z większej ilości miejsca w tej usłudze.

76. Apple deklaruje, że usługa iCloud została opracowana przy użyciu „standardowych w branży technologii" zabezpieczeń i obowiązują w niej rygorystyczne zasady związane z ochroną informacji.[104]

77. Apple również wprowadza rozróżnienie na szyfrowanie „w spoczynku" i „w trakcie przesyłu".

78. Co jednak ciekawe Apple wskazuje, że dane w usłudze iCloud Mail nie są szyfrowane podczas ich przechowywania na serwerze („w spoczynku"). Według wyjaśnień Apple: „Zgodnie ze standardowymi w branży metodami postępowania usługa iCloud nie szyfruje danych przechowywanych na serwerach poczty IMAP."[105]

79. W przypadku pozostałych dostawców informacji o różnicy w szyfrowaniu wynikającej z korzystania z serwerów poczty IMAP jednak nie odnaleźliśmy. Weryfikacja znaczenia tej informacji dla

[102] Zob. więcej https://docs.microsoft.com/en-us/microsoft-365/compliance/ome?view=o365-worldwide, dostęp na dzień 14 czerwca 2020 r.

[103] https://docs.microsoft.com/en-us/microsoft-365/compliance/email-encryption?view=o365-worldwide#comparing-email-encryption-options-available-in-office-365, dostęp na dzień 14 czerwca 2020 r.

[104] https://support.apple.com/pl-pl/HT202303, dostęp na dzień 14 czerwca 2020 r.

[105] https://support.apple.com/pl-pl/HT202303, dostęp na dzień 14 czerwca 2020 r.

potencjalnego poziomu bezpieczeństwa wiadomości e-mail przechowywanych przez radców prawnych wymagałaby uzyskania bardziej szczegółowych informacji od Apple.

80. Apple zamieszcza następujące informacje dotyczące zabezpieczeń przechowywanych danych[106]:

> Do przechowywania takich danych osobowych Apple stosuje systemy komputerowe z ograniczonym dostępem znajdujące się w fizycznie zabezpieczonych pomieszczeniach. Z wyjątkiem usługi iCloud Mail dane w ramach usługi iCloud są przechowywane w formie zaszyfrowanej także wtedy, gdy Apple korzysta z zewnętrznych rozwiązań w zakresie przechowywania danych.

81. W innym miejscu Apple informuje, że[107]:

> W niektórych przypadkach dane iCloud mogą być przechowywane przy użyciu serwerów należących do partnerów zewnętrznych, takich jak Amazon Web Services lub Google Cloud Platform, jednak partnerzy ci nie mają kluczy umożliwiających odszyfrowanie danych przechowywanych na ich serwerach.

82. Biorąc pod uwagę te dwie informacje trudno rozstrzygnąć, czy dane przechowywane w usłudze iCloud Mail są szyfrowane, gdy Apple przechowuje je na zewnętrznych serwerach (np. w Google Cloud), czy nie. Również w tym przypadku należałoby zwrócić się do Apple z prośbą o dodatkowe wyjaśnienia.

83. W spoczynku są szyfrowane dane przechowywane w ramach kopii zapasowych. Apple stosuje w tym przypadku co najmniej szyfrowanie AES z kluczem 128-bitowym.[108]

84. Jeśli chodzi o dane „w trakcie przesyłu", to w tym przypadku Apple jednoznacznie deklaruje, że „cały ruch między urządzeniami a usługą iCloud Mail jest szyfrowany przy użyciu technologii TLS 1.2".[109] Systemy operacyjne urządzeń Apple obsługują TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3.[110]

85. Analogicznie jak w przypadku Google i Microsoft, szyfrowanie danych „w trakcie przesyłu" oznacza, że zabezpieczone jest połączenie od urządzenia użytkownika do serwerów dostawcy usługi.

86. Jeżeli użytkownik korzysta z programu pocztowego Apple, to ma możliwość skorzystania z rozszerzonego standardu szyfrowania S/MIME.[111] Standard ten Apple obsługuje także dla

---

[106] https://www.apple.com/legal/privacy/pl/, dostęp na dzień 14 czerwca 2020 r.
[107] https://support.apple.com/pl-pl/HT202303, dostęp na dzień 14 czerwca 2020 r.
[108] https://support.apple.com/pl-pl/HT202303, dostęp na dzień 14 czerwca 2020 r.
[109] https://support.apple.com/pl-pl/HT202303, dostęp na dzień 14 czerwca 2020 r.
[110] https://support.apple.com/pl-pl/guide/security/sec100a75d12/web, dostęp na dzień 14 czerwca 2020 r.
[111] https://support.apple.com/pl-pl/HT202303, dostęp na dzień 14 czerwca 2020 r.

pojedynczych wiadomości. Użytkownik ma więc możliwość ustawienia, że podpisywane i szyfrowane w ten sposób będą wszystkie wiadomości lub jedynie wybrane e-maile.

87. Apple posiada ciekawą możliwość tzw. „kompleksowego szyfrowania danych", która oznacza, że dostęp do danych ma jedynie użytkownik i nawet Apple nie może odczytać danych zaszyfrowanych w tym modelu (jest to więc to model „zero-knowledge encryption"). Z informacji zamieszczonych przez Apple nie wynika jednak by szyfrowanie kompleksowe obejmowało usługę iCloud Mail.[112]

Rekomendacje

88. Wszyscy dostawcy poczty elektronicznej, o których mowa wyżej, deklarują, że stosują odpowiednie środki i standardy bezpieczeństwa pozwalające chronić poufność danych. Deklarują również, że stosują szyfrowanie poczty, chociaż ich oświadczenia różnią się co do szczegółów.

89. W naszej ocenie deklaracje Google i Microsoft dotyczące standardowo stosowanych metod szyfrowania danych „w spoczynku" są zbliżone. Oba podmioty szyfrują dane przy użyciu szyfrowania Advanced Encryption Standard (AES). Google oświadcza, że jest to klucz 128-bitowy lub silniejszy. W przypadku Microsoft, zapewnienie poufności danych również odbywa się przy pomocy AES (128-bitowego lub 256-bitowego). Jak się wskazuje przy omawianiu szyfru AES, klucz „128-bitowy jest najbardziej popularny, ponieważ sprawia, że szyfrowanie jest nieco szybsze, a różnica między bezpieczeństwem 128- a 256-bitowym jest bez znaczenia dla większości aplikacji."[113]

90. W przeciwieństwie do Google i Microsoft, Apple oświadcza, że nie szyfruje poczty elektronicznej w przypadku gdy dane znajdują się „w spoczynku". Apple twierdzi, że brak szyfrowania danych przechowywanych na serwerach poczty IMAP jest standardem w branży. Jak jednak już wspomniano, Google i Microsoft nie czynili takiego rozróżnienia, dlatego kwestia ta wymagałaby dalszej weryfikacji i zadania dodatkowych pytań Apple.

91. Jeżeli chodzi o szyfrowanie danych „w trakcie przesyłu" deklaracje wszystkich trzech dostawców są zbliżone i opierają się na wskazaniu, że usługa obejmuje możliwość korzystania z TLS. Wszyscy dostawcy zapewniają możliwość korzystania z dodatkowych sposobów ochrony wiadomości, w tym m.in. przez wykorzystanie standardu S/MIME.

92. W naszej ocenie – opartej na oświadczeniach dostawców – korzystanie z Gmaila (w ramach pakietu G Suite) i usługi Exchange Online spełnia wymogi bezpieczeństwa, które powinny obowiązywać radców prawnych. W kwestii usługi iCloud Mail, z uwagi na niejednoznaczność

[112] https://support.apple.com/pl-pl/HT202303, dostęp na dzień 14 czerwca 2020 r.
[113] Jean-Philippe Aumasson, *Nowoczesna kryptografia,* Wydawnictwo Naukowe PWN, 2018, str. 105.

informacji przekazanych przez Apple, ostrożnie wstrzymujemy się z wydaniem opinii, ponieważ, naszym zdaniem, potrzebne byłoby uzyskanie dodatkowych informacji od Apple. Być może nie ma tutaj podstaw do uznania, że standard Apple jest niższy od standardów innych dostawców.

93. Trzeba również podkreślić to, że niezależnie od stosowanych standardów szyfrowania, wszyscy trzej omówieni dostawcy są globalnymi podmiotami. Z uwagi na wielkość organizacji i posiadane środki finansowe, są one w stanie zapewnić poziom bezpieczeństwa, który w praktyce trudno osiągnąć samodzielnie w kancelarii prawnej bez ponoszenia bardzo dużych kosztów.

94. Przede wszystkim więc radca prawny wybierający usługodawcę, powinien zweryfikować postanowienia regulaminu i sprawdzić, czy nie ma w nim postanowień, które wykluczają stosowanie tej usługi lub przynajmniej budzą wątpliwości z punktu widzenia potencjalnej ochrony danych. Wybrany powinien zostać dostawca, którego deklaracje dotyczące standardów bezpieczeństwa nie odstają od praktyki rynkowej i który (choć to czynnik bardziej subiektywny) jest dla radcy prawnego wiarygodny. Kwestię wiarygodności można zweryfikować chociażby przez sprawdzenie, czy w historii działalności dostawcy zdarzały się na przykład wycieki danych lub też przez analizę informacji dotyczących podejścia danego dostawcy do prywatności.

95. Jeżeli zaś chodzi o samo korzystanie z poczty elektronicznej, to w naszej ocenie radca prawny powinien poinformować klienta o potencjalnych zagrożeniach związanych z korzystaniem z tego środka komunikacji, w szczególności w przypadku braku szyfrowania.

96. Z opinii American Bar Association wynika, że nieszyfrowane e-maile nie powodują powstania większego ryzyka przechwycenia lub ujawnienia niż inne nieelektroniczne formy komunikacji oraz że korzystanie z nieszyfrowanych maili w rutynowych przypadkach pozostaje akceptowalną metodą komunikacji z klientami.[114]

97. Ogólnie podzielamy takie stanowisko, choć w naszej ocenie korzystanie z TLS powinno być standardem – przynajmniej po stronie radców prawnych. Korzystanie z tego protokołu nie powoduje bowiem w zasadzie żadnych trudności w komunikacji, a może poprawić bezpieczeństwo połączenia.

98. Radca prawny powinien więc w każdym przypadku korzystać z protokołu TLS i zarekomendować klientowi, by również korzystał z tego protokołu. Mamy jednak świadomość, że w praktyce przekonanie klientów do stosowania takiego zabezpieczenia może stanowić wyzwanie. O ile jeszcze w przypadku klientów biznesowych może nie być z tym problemów, to konsumenci

[114] American Bar Association, *Formal Opinion 477R*, 11 maja 2017 r., zmieniona 22 maja 2017 r., https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.pdf, dostęp na dzień 11 czerwca 2020 r.

w większości używają przecież darmowych skrzynek mailowych i mogą nie mieć wiedzy w tym zakresie.

99. W przypadku najbardziej „wrażliwych” informacji przesyłanych pocztą elektroniczną (np. posiadających dużą wartość gospodarczą), rekomendowalibyśmy aby radcowie prawni rozważyli stosowanie dodatkowych metod szyfrowania jak PGP czy S/MIME. Zdajemy sobie sprawę, że w codziennej komunikacji takie rozwiązania mogą być z praktycznych względów kłopotliwe. Jednak podjęcie dodatkowych środków bezpieczeństwa w niektórych przypadkach będzie z pewnością uzasadnione.

100. Być może warto byłoby opracować dla radców prawnych krótki poradnik wyjaśniający jak należy stosować tego rodzaju szyfrowanie w najbardziej popularnych programach pocztowych, co niniejszym poddajemy pod rozwagę.

101. Na koniec wskazujemy, że najprostsza ochrona przesyłanych drogą elektroniczną dokumentów, czyli ochrona hasłem załączników, również może być warta rozważenia.

102. Nie jest to rozwiązanie pozbawione wad, ponieważ wymaga pamiętania (zapisywania) różnych haseł dla różnych klientów.

103. W przypadku utraty hasła dostęp do załącznika może być niemożliwy. Jednak w przypadku gdy e-mailem przesyłane są dokumenty zawierające szczególnie poufne informacje, ochrona hasłem powinna być standardem.

104. Przy wysyłaniu kilkudziesięciu wiadomości dziennie nietrudno przecież o pomyłkę przy wpisywaniu adresata, która może spowodować, że załącznik zawierający informacje o szczególnej wartości trafi w niepowołane do tego ręce.

radca prawy Damian Nartowski radca prawny Karol Wątrobiński