KSIĘGA BEZPIECZEŃSTWA KOMUNIKACJI ELEKTRONICZNEJ W PRACY RADCY PRAWNEGO. CZĘŚĆ 2

PROGRAMY POCZTOWE W PRACY RADCY PRAWNEGO

KRAJOWA IZBA
RADCÓW PRAWNYCH

Ocena zgodności Exchange Online, Gmail, iCloud Mail dla celów działalności radców prawnych

Spis treści

Gawroński & Partners S.K.A.
info@gppartners.pl
al. Jana Pawła II 12
00-124 Warszawa

Warszawa, 21 sierpnia 2020

Dotyczy: Ocena zgodności Exchange Online, Gmail, iCloud Mail dla celów działalności radców prawnych

Przedstawiamy opinię prawną dotyczącą oceny zgodności usług poczty elektronicznej:

1) **Exchange Online w ramach Microsoft 365**, formalnie oferowanej dla firm z Europejskiego Obszaru Gospodarczego przez Microsoft Ireland Operations Limited
2) **Gmail w ramach G-Suite** formalnie oferowanej dla firm z Europejskiego Obszaru Gospodarczego przez Google Ireland Limited[1]
3) **iCloud Mail w ramach Apple Business Manager** formalnie oferowanej dla firm z Europejskiego Obszaru Gospodarczego przez Apple Distribution International Ltd. z siedzibą przy Holly Industrial Estate, Hollyhill, Cork, Irlandia;

dla potrzeb wykonywania zawodu przez radców prawnych w formie kancelarii radcy prawnego.

Analizę oparliśmy na naszym autorskim podziale funkcjonalnym RODO na trzy filary: legalność, prawa jednostki i bezpieczeństwo, oraz dwa fundamenty: rozliczalność i ocenę ryzyka, zaproponowanym w książkach „RODO. Przewodnik ze wzorami" (s. 32), „Ochrona Danych Osobowych. Przewodnik po Ustawie i RODO z wzorami" (s. 46), „Guide to the GDPR" (s. 6). Schemat oceny zbieżny jest z zastosowanym w naszej opinii z dnia 31 maja 2020 r. dotyczącej oceny zgodności wykorzystywania usług wideokonferencyjnych Teams, Zoom, Webex w działalności radców prawnych.

Oceniamy zgodność z prawem (legalność) i bezpieczeństwo przetwarzania danych w usługach poczty elektronicznej oferowanych przez Dostawców. Nie oceniamy jedynie kwestii realizacji praw jednostki (praw osób, których dane dotyczą), ze względu na to, że główna relacja pomiędzy radcą prawnym a dostawcą usługi jest relacją powierzenia przetwarzania danych, a podmiot przetwarzający pełni w odniesieniu do obsługi praw jednostki tylko rolę pomocniczą dla administratora danych. Niniejsza opinia jest narzędziem zapewniającym realizację zasady rozliczalności, a w jej treść wplatamy elementy oceny ryzyka, w ten sposób wypełniając wszystkie pięć elementów podziału funkcjonalnego RODO. Oceniając bezpieczeństwo, koncentrujemy się na poufności, w ten sposób konsumując też ocenę możliwości zapewnienia przez radcę tajemnicy zawodowej.

Nasza opinia przedstawia:

(i) obowiązki radców prawnych wynikające z przepisów prawa w związku z korzystaniem z usług poczty elektronicznej

(ii) opis omawianych usług poczty elektronicznej

(iii) analizę zgodności z przepisami prawa dla każdej usługi

(iv) ogólne wnioski i wskazówki dla radców płynące z analizy.

Opinia i zawarta w niej analiza zgodności bazuje na dokumentach i źródłach powszechnie dostępnych dla każdej z usług oferowanych przez Dostawców.

I. PODSUMOWANIE

Przeprowadzona przez nas analiza doprowadziła nas do następujących wniosków.

1) Radcowie prawni mogą wykorzystywać dla celów wykonywania zawodu usługi Exchange Online w ramach pakietu Microsoft 365 a także Gmail w ramach pakietu G-Suite, natomiast wątpliwe byłoby wykorzystywanie usługi iCloud Mail.

[1] Wersja umowy na usługi G Suite dostępna w procesie rejestracji usługi domyślnie wskazuje podmiot z siedzibą w Irlandii jako dostawcę usług: https://admin.google.com/terms/apps/1/11/en/premier_terms_eea.html

2) Warunkiem legalności korzystania z którejkolwiek z usług dla celów wykonywania zawodu jest wykupienie usługi biznesowej przez radcę.

   Umowa powierzenia przetwarzania danych dotycząca korzystania z usług poczty email dostępna jest tylko w wersji biznesowej usługi. Użytkownicy korzystający z usługi dla potrzeb prywatnych, co do zasady nie są administratorami danych i w związku z tym nie powierzają danych do przetwarzania dostawcy.

3) Wszystkie usługi email zapewniają wysoki poziom bezpieczeństwa (poufności i ciągłości), niemożliwy do osiągnięcia przez radcę w wersji „on premise", tym bardziej przy porównywalnych kosztach dla mikro lub małej firmy.

4) Warunki prawne Microsoft 365 i G-Suite są zgodne z wymaganiami RODO (przy tym potwierdzenie zgodności G-Suite wymaga nieco interpretacji) natomiast warunki prawne usługi Apple Business Manager trudno jednoznacznie uznać za zgodne z RODO.

5) W Microsoft 365 dane (korespondencja) są przechowywane na terenie Europejskiego Obszaru Gospodarczego (**EOG**), w G-Suite można (i należy) ustawić przechowywanie danych w EOG, natomiast w iCloud przechowywanie danych nie może zostać ograniczone do EOG.

   Ograniczenie przechowywania emaili do terenu EOG w usługach Microsoft 365 (Exchange Online) i G-Suite (Gmail) w naszej ocenie pozwala uznać, że dane osobowe w tych usługach są chronione odpowiednio.

   Co do iCloud Mail, na tle treści wyroku Schrems II ocena ryzyka naruszenia praw i wolności osób, których dotyczyłaby korespondencja email radcy, może doprowadzić do uznania, że dane te nie będą w usłudze iCloud podlegały ochronie odpowiedniej do ochrony wynikającej z prawa UE (RODO).

6) **Microsoft.** W celu legalnego korzystania z usługi poczty Microsoft Exchange Online nic nie trzeba robić – przeciwnie NIE NALEŻY zmieniać ustawień przy tzw. „Geo", czyli domyślnym dla użytkowników z EOG (po angielsku *European Economic Area* = EEA) ustawieniu ograniczenia przechowywania danych do regionu EOG.

7) **Google.** Radca prawny korzystający z wersji biznesowej Gmail (w ramach pakietu G-Suite) dodatkowo powinien zaakceptować umowę powierzenia oraz wybrać region „Europa", w którym przechowywane będą dane (wybór regionu przechowywania danych możliwy jest tylko w wersji G Suite Business oraz G Suite Enterprise). Zarówno umowy związane z przetwarzaniem danych jak i wybór regionu przechowywania danych znajdują się w sekcji konsoli administratora Google G-Suite: KONTO => USTAWIENIA KONTA.

   Zgodnie z komunikatem Google rozesłanym użytkownikom 11 sierpnia 2020, nie ma już konieczności odrębnej akceptacji standardowych klauzul umownych (**SCC**) (w umowie przetwarzania danych Google, czyli *Data Processing Amendment* = *DPA*, nazywane *Model Contract Clauses* = *MCC*).

8) **Apple.** Apple nie umożliwia ograniczenia przechowywania danych (emaili) do EOG. Z tego powodu, a także w związku z daleko idącymi uprawnieniami, jakie Apple przyznaje sobie względem danych powierzonych, a także wobec niskiej transparentności prawnych warunków przetwarzania danych, korzystanie z usługi iCloud dla celów profesjonalnych przez radców prawnych jest dyskusyjne.

9) **Transfer danych do USA.** Wszyscy dostawcy transferują do USA obecnie dane telemetryczne i dane podstawowe użytkowników, na podstawie SCC. Oceniając to na tle wyroku TSUE „Schrems II", uważamy, że SCC zasadniczo zapewniają odpowiednią (do UE) ochronę danych innych niż kontent przy transferze do USA. Potwierdzają to statystyki nakazów USA (FISA[2] i NSL[3]), do których odwołuje się NOYB (fundacja Maxa Schremsa), a z których wynika, że ilość żądań niedotyczących kontentu jest pomijalna[4].

[2] Foreign Intelligence Surveillance Act
[3] national security letters
[4] https://noyb.eu/en/next-steps-eu-companies-faqs

10) **Dostawca chmurowy jako administrator.** Microsoft i Apple rozpoznają swoją rolę jako administratora danych telemetrycznych i danych o użytkownikach. Nie wyklucza to naszym zdaniem korzystania z usług dostawców poczty, którzy widzą się wyłącznie w roli podmiotów przetwarzających (tu Google). Wnioski z opinii wideokonferencyjnej pozostają tu aktualne.

Podsumowując:

Niedopuszczalne jest korzystanie z darmowych wersji omawianych usług, gdyż dostawcy dla takiej wersji usługi nie oferują umowy powierzenia przetwarzania danych.

Poczta Microsoft 365 (Exchange Online) jest najłatwiejsza do obsługi „regulacyjnej" i uzasadnienia zgodności.

Gmail ma najsłabszą reputację w odniesieniu do ochrony prywatności, ale przy spełnieniu wskazanych w opinii wymagań wydaje się zapewniać zgodność. Istotny jest wybór wersji pakietu G Suite. Najtańsza opcja G Suite Basic nie daje możliwości wyboru regionu przechowywania danych, dlatego rekomendowane jest korzystanie z wersji G Suite Business, G Suite Enterprise lub G Suite Enterprise Essentials.

Apple ma najlepszą reputację w ochronie prywatności, ale trudno uznać za zgodne z RODO prawne warunki Apple przetwarzania danych dla klientów biznesowych, oraz nie można ograniczyć przechowywania emaili w iCloud Mail do EOG, co łącznie naszym zdaniem co do zasady wyklucza obecnie dopuszczalność używania iCloud Mail do wykonywania zawodu przez radców prawnych.

II. Natura i prawne aspekty usługi poczty elektronicznej

1. Usługa poczty elektronicznej

Każdy z Dostawców – Microsoft, Apple oraz Google oferuje swoim klientom szereg usług ułatwiających prowadzenie działalności biznesowej. Z uwagi na skalę działalności Dostawców, przetwarzaną przez nich ilość danych i oczywiście aktualne uwarunkowania technologiczne, usługi oferowane przez Dostawców świadczone są z wykorzystaniem chmury obliczeniowej.

Jedną z podstawowych usług oferowanych przez Dostawców w ramach prowadzonych przez nich działalności jest usługa poczty elektronicznej (**usługa email**).

Usługa email polega na dostarczaniu funkcjonalności serwera poczty elektronicznej oraz (ewentualnie) umożliwieniu dostępu do poczty elektronicznej przez przeglądarkę internetową. Dostarczanie aplikacji (klient poczty) pozwalającej obsługiwać pocztę elektroniczną na komputerze lub innym terminalu nie jest dostarczaniem usługi email. W opinii koncentrujemy się na funkcjonalności serwera poczty email.

Upraszczając maksymalnie, poczta elektroniczna to usługa przechowywania danych (emaili), wysyłania danych (emaili) i odbierania danych (emaili).

2. Cel korzystania z poczty elektronicznej przez radców

Opinia analizuje zgodność z prawem korzystania przez radców prawnych z usług email oferowanych przez Google, Apple oraz Microsoft w celu wykonywania zawodu, w tym:

1) świadczenia pomocy prawnej w tym kontaktowania się z klientami w sprawach objętych tajemnicą zawodową;
2) kontaktowania się za pomocą poczty elektronicznej z dostawcami, pracownikami i współpracownikami kancelarii;
3) organizacji pracy wewnątrz kancelarii, w tym organizacji i przechowywania dokumentów zawierających tajemnicę zawodową radcy prawnego;

3. Prawne aspekty usługi email

Poczta elektroniczna jest usługą internetową, która zgodnie z UŚUDE (art. 1 pkt 4) jest tzw. usługą świadczoną drogą elektroniczną, tj. usługą świadczoną 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 (na odległość).

Z perspektywy UŚUDE poczta elektroniczna kwalifikuje się jako rodzaj tzw. hostingu, czyli usługi przechowywania danych, o której mowa w art. 14 UŚUDE.

Z perspektywy RODO, świadczenie usługi email jak i korzystanie z niej wiąże się z przetwarzaniem różnego rodzaju informacji, w tym danych osobowych.

Zgodnie z art. 4 pkt 2) RODO, przetwarzanie danych osobowych to: *operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak **zbieranie**, utrwalanie, organizowanie, porządkowanie, **przechowywanie**, adaptowanie lub modyfikowanie, **pobieranie**, **przeglądanie**, wykorzystywanie, **ujawnianie poprzez przesłanie**, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie*.

Kategorie danych. Dane osobowe przetwarzane w ramach poczty elektronicznej można skategoryzować następująco:

- **podstawowe i kontaktowe dane użytkownika**: imię, nazwisko, email, telefon, login, hasło, organizacja, metoda płatności, ustawienia preferencji;
- **treści/kontent:** czyli dane przechowywane i przesyłane przez użytkowników – treść maili oraz wszelkie możliwe załączniki (pliki) dołączone do maili oraz wszelkie możliwe dane i pliki przechowywane i udostępniane w ramach usług. Treści/kontent mogą zawierać „wszystko" czyli także dane szczególnych kategorii lub dane „karne" (tzw. dane nieustrukturyzowane) jak również listę kontaktów, która stanowi uporządkowany zbiór danych osobowych o odbiorcach poczty elektronicznej, nieustrukturyzowane dane kontaktowe przesyłane w ramach kontentu
- **dane techniczne / telemetryczne**: IP, lokalizacja i cechy sprzętu, natężenie ruchu, requesty (czyli techniczne żądania wysyłane przez użytkownika do serwera poczty, typu: wyślij, przeorganizuj, ustaw regułę serwerową), anomalie (anomalia to rodzaj metadanych, czyli wniosek, że pewne dane odbiegają od normy), itp;
- **dane drugiej strony korespondencji:** dane identyfikacyjne (nieuwierzytelnione lub uwierzytelnione, w zależności od użytych protokołów komunikacji), dane telemetryczne.

W konsekwencji, korzystanie z usługi email wiąże się z następującymi zagadnieniami prawnymi dotyczącymi przetwarzania danych osobowych oraz przetwarzania tajemnic za pomocą podmiotów trzecich[5]:

(1) rola i pozycja dostawcy usługi poczty elektronicznej względem usługobiorcy (radcy) – 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 – zmiany od 16 lipca 2020

(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 świadczenia usług drogą elektroniczną, czyli przede wszystkim formalny obowiązek sporządzenia odpowiedniego:

[5] 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 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

(7) regulaminu usługi (przez podmiot, który oferuje daną usługę)

– tu od razu informujemy, że radca nie musi posiadać regulaminu komunikacji emailowej[6].

4. Transfer danych do USA – RODO przed wyrokiem Schrems II

Radca prawny korzystający z poczty elektronicznej jest zobowiązany do weryfikacji, czy dane przetwarzane przez dostawcę poczty elektronicznej nie są przekazywane poza EOG. Przekazywanie danych poza EOG wiąże się z dodatkowymi obowiązkami nałożonymi na administratorów, w tym weryfikacji podstawy prawnej do takiego transferu poza EOG. Nie chodzi tu oczywiście o sam proces przesyłania danych na linii urządzenie nadawcy => serwer email nadawcy => serwer email adresata => urządzenie adresata[7], tylko o to, gdzie serwer email przechowuje dane nadane i odebrane.

Przekazywanie danych osobowych poza terytorium Europejskiego Obszaru Gospodarczego zostało uregulowane w rozdziale V RODO. Taki „eksport danych" wymaga odrębnej (dodatkowej) niż art. 6 lub art. 9 RODO podstawy prawnej.

W praktyce przekazywanie danych osobowych do Stanów Zjednoczonych, skąd pochodzą omawiani przez nas dostawcy usług email, odbywało się na dwóch podstawach prawnych (często wspólnie):

(1) tak zwana Tarcza Prywatności (*Privacy Shield*)

(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.

4.1. Privacy Shield / Tarcza Prywatności

Zgodnie z 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.*

Microsoft oraz Google widnieją na liście podmiotów objętych programem Tarczy Prywatności UE-USA. Apple nie dokonał samocertyfikacji w ramach Programu Tarczy Prywatności UE-USA.

Jednak od 16 lipca 2020 r. transfer danych osobowych do USA na podstawie decyzji w sprawie Tarczy Prywatności jest nielegalny (wyrok Schrems II, o którym dalej). W konsekwencji, aby korzystać z usług poczty elektronicznej oferowanej przez dostawcę, który transferuje dane do Stanów Zjednoczonych, należy poszukiwać innej podstawy legalizującej taki transfer danych.

4.2. Standardowe klauzule umowne

Inną podstawą transferu danych poza EOG może być stosowanie tzw. standardowych klauzul umownych (SCC, standard contractual clauses, model EU contract clauses) w umowie pomiędzy administratorem danych w EOG a odbiorcą danych poza EOG.

SCC to wzorce konkretnych zobowiązań umownych pomiędzy administratorem danych wysyłającym dane poza UE a odbiorcą (administratorem lub podmiotem przetwarzającym) tych danych poza UE, zatwierdzone decyzją Komisji Europejskiej. Zawarcie SCC dotychczas wystarczało do uznania, że transfer danych osobowych poza UE na ich podstawie zapewniał odpowiedni poziom ochrony danych.

Zgodnie z 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.*

---

[6] Ale zobaczymy co jeszcze UE wymyśli.

[7] Przesył pakietów danych jest domeną prawa telekomunikacyjnego. W praktyce odbywa się z pomocą urządzeń na całym świecie (w technologii MPLS de facto korzystającej ze światowego internetu)

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;*

Wszyscy omawiani dostawcy oferują SCC dla swoich usług email. Jednak wyrok w sprawie Schrems II odnosi się również do możliwości „eksportu" danych poza EOG na podstawie standardowych klauzul umownych (SCC).

5. Schrems II

W dniu 16 lipca 2020 r. Trybunał Sprawiedliwości Unii Europejskiej (TSUE) wydał wyrok w sprawie C-311/18[8], (dalej: **Schrems II**)[9], w którym na tle transferu danych między Facebook Ireland a Facebook Inc. TSUE wypowiedział się co do ważności „eksportu" danych poza EOG na podstawie: **(i)** decyzji Komisji Europejskiej w sprawie tzw. Tarczy Prywatność oraz na podstawie **(ii)** tak zwanych standardowych klauzul umownych (SCC).

5.1. Nieważność Tarczy Prywatności

Komisja w dniu 12 lipca 2016 r przyjęła decyzję w sprawie odpowiedniej ochrony danych osobowych dla programu Tarcza Prywatności UE-USA („**Privacy Shield**"). Privacy Shield wprowadzała możliwość tak zwanej samocertyfikacji podmiotów ze Stanów Zjednoczonych na zgodność z prawem ochrony danych EU. Samocertyfikacja polega na złożeniu 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).

W wyroku Schrems II TSUE uznał za nieważną Decyzję Komisji Europejskiej w sprawie Privacy Shield. Podstawowym argumentem podnoszonym przez TSUE jest brak proceduralnych gwarancji dla osób spoza USA poddawanych masowej inwigilacji elektronicznej na podstawie amerykańskiego prawodawstwa[10].

TSUE unieważnił Tarczę Prywatności podnosząc w zasadzie te same argumenty co w tzw. wyroku Schrems I z 6 października 2015 (sprawa C-362/14), którym TSUE unieważnił tzw. Bezpieczną Przystań – poprzedniczkę Tarczy Prywatności. TSUE ponownie wskazał na brak proceduralnych gwarancji dla osób spoza USA poddawanych masowej inwigilacji elektronicznej na podstawie amerykańskiego prawodawstwa. Trzy główne amerykańskie akty prawne poddane krytyce to ustawa o kontroli wywiadu zagranicznego (FISA), rozporządzenie wykonawcze 12333 i dyrektywa polityczna Prezydenta nr 28. W ocenie TSUE uprawnienia amerykańskich agend rządowych wynikające z prawodawstwa amerykańskiego względem „danych zagranicznych" są tak duże i tak niekontrolowane, że nie sposób uznać, że Tarcza Prywatności rzeczywiście dawała rezydentom Unii Europejskiej ochronę odpowiednią do ochrony danych w EU. Sąd wskazał, że prawo amerykańskie inaczej (dużo bardziej) chroni obywateli amerykańskich, nie dając porównywalnych, a w zasadzie żadnych gwarancji ochrony prawnej przed inwigilacją osobom spoza USA. W konsekwencji od 16 lipca 2020 wszelki transfer danych na podstawie Tarczy Prywatności jest **nielegalny**[11].

5.2. Względność standardowych klauzul umownych

Oprócz unieważnienia Tarczy Prywatności, TSUE wypowiedział się też na temat skuteczności standardowych klauzul umownych, dopuszczalności i legalności przesyłania na ich podstawie danych osobowych poza Europejski Obszar Gospodarczy.

TSUE w wyroku Schrems II wskazał, że legalność transferu danych w oparciu o SCC należy badać na tle prawodawstwa państwa docelowego. Jeżeli prawodawstwo to nie zapewnia odpowiednich

---

[8] Treść wyroku: http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=10402470

[9] Nazwa wyroku pochodzi od nazwiska austriackiego aktywisty Maxa Schremsa, który doprowadził do tego orzeczenia.

[10] Więcej na temat: https://gppartners.pl/pl/co-z-uslugami-chmurowymi-po-wczorajszym-wyroku-tsue-uniewazniajacym-transfery-do-usa/

[11] https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en

proceduralnych gwarancji dla podmiotów danych (rezydentów UE) i dopuszcza dowolny dostęp do tych danych agendom rządowym państwa docelowego, to nie można uznać, że ochrona danych zapewniana przez zawarte SCC będzie miała stopień odpowiedni do europejskiego. A w konsekwencji taki transfer pozostanie nielegalny lub może za taki zostać uznany przez organ nadzorczy i zakazany.

W powiązaniu z ustaleniami dotyczącymi uprawnień do inwigilacji cudzoziemców, które USA sobie przyznało, i braku obronnych narzędzi proceduralnych dla inwigilowanych cudzoziemców, stanowisko TSUE oznacza, że SCC same w sobie przestały być samodzielną podstawą do przesyłania danych osobowych z UE do USA. Każdy przypadek przesyłania danych osobowych do USA stał się „podejrzany" i należy zweryfikować realną adekwatność ochrony danych przy takim transferze. W praktyce TSUE zlikwidował automatyzm przesyłania danych do USA na podstawie SCC.

W dalszej części opinii przedstawiamy naszą ocenę legalności korzystania z omawianych chmurowych usług email z uwzględnieniem wyroku Schrems II. Ocena ta wypada korzystnie dla Microsoft i Google, natomiast niekorzystnie dla Apple.

6. Radca prawny – administrator czy podmiot przetwarzający?

Klient administrator, dostawca przetwarzający. Dostawca usługi poczty elektronicznej jest zasadniczo 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). Dostawcy usług identyfikują siebie jako podmioty przetwarzające na zlecenia klienta.

Radca jako administrator. Zgodnie z dominującym podglądem, radca prawny wykonujący zawód w formie kancelarii radcy prawnego jest administratorem danych osobowych przetwarzanych w ramach wykonywania zawodu. Pogląd ten potwierdzony został w znowelizowanej Ustawie o radcach prawnych, w ten sposób, że obowiązki, do których odnoszą się przepisy rozdziału 1a Ustawy o radcach prawnych (w tym obowiązek odpowiadania na żądania z art. 15, 18, 19 i 21 RODO) są nałożone właśnie na administratora danych osobowych.

Mogą zdarzyć się również sytuacje, gdy radca prawny będzie występował w charakterze podmiotu przetwarzającego. Np. gdy kancelaria świadczy usługi na rzecz dużego klienta korporacyjnego, takie było życzenie tego klienta, a kancelaria zamiast „kopać się z koniem" po prostu podpisała umowę powierzenia. Konsekwencje takiej sytuacji również omawiamy w kolejnym rozdziale – **Obowiązki radców korzystających z usługi email**.

Dostawca jako administrator. W praktyce w pewnym zakresie dostawca usługi email działa też jako administrator niektórych danych osobowych pozyskanych w związku z korzystaniem z usługi przez jej użytkowników[12]. Chodzi tu przede wszystkim o wspominane dane techniczne/telemetryczne i podstawowe dane użytkownika, dla celów zarządzania użytkownikami, raportowania finansowego oraz cyberbezpieczeństwa.

Brak współadministrowania. W naszej ocenie w żadnym zakresie nie powstaje pomiędzy klientem a dostawcą usługi stosunek współadministrowania danymi osobowymi. To stwierdzenie jest istotne ze względu na kontrowersyjny wyrok Trybunału Sprawiedliwości UE z dnia 29 lipca 2019[13] 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.

[12] Dostawca usług jest też administratorem danych osobowych pozyskiwanych od swoich klientów konsumenckich, co jednak pozostaje poza zakresem zainteresowania naszej opinii.

[13] http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=1278754

III. OBOWIĄZKI RADCÓW KORZYSTAJĄCYCH Z USŁUGI EMAIL

1. Radca jako administrator

Klient usługi email (radca prawny) będąc administratorem danych, zawierając umowę z dostawcą usługi email ma następujące obowiązki z obszaru ochrony danych osobowych i Ustawy o radcach prawnych:

1) **[tajemnica zawodowa]** 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. obowiązek zachowania tajemnicy zawodowej obejmuje również wszelkie tworzone przez radcę prawnego dokumenty oraz korespondencję radcy prawnego z klientem i osobami uczestniczącymi w prowadzeniu sprawy, w tym komunikację w ramach emalii oraz dokumenty przetwarzane w chmurze obliczeniowej.

2) **[wiarygodność]** radca prawny powinien 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:

   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.

   Chodzi tu o weryfikację:

   a) zgodności działania usługi z prawem ochrony danych osobowych

   b) odpowiedniego bezpieczeństwa usługi

   Sprawdzenia „wystarczających gwarancji" 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 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 w dalszej części opinii.

3) **[umowa powierzenia]** radca prawny powinien 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.

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

   Każdy z omawianych dostawców usług email pochodzi z USA i „jakieś" dane do USA przekazuje.

   Po wyroku Schrems II transfer danych do USA można oprzeć w praktyce tylko na Standardowych Klauzulach Umownych. Trzeba przeprowadzić jednak dodatkową analizę ryzyka.

5) **[obowiązek informacyjny]** należy informować osoby, z którymi prowadzimy korespondencję mailową, o tym, w jaki sposób przetwarzane są ich dane osobowe w związku z korzystaniem przez radcę z danej usługi (art. 13 RODO).

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

7) **[retencja danych]** należy też w swojej polityce retencji danych uwzględnić proces przetwarzania danych w ramach poczty elektronicznej i wskazać, przez jaki okres maile będą przechowywane w ramach poczty elektronicznej[14].

Niniejsza opinia jest istotnym narzędziem do „rozliczenia się" z RODO (obowiązek wskazany w ppkt 6 powyżej) i z obowiązku zachowania tajemnicy zawodowej w zakresie omawianych nią usług email.

2. Radca jako podmiot przetwarzający

Jak wskazaliśmy wyżej, może zdarzyć się, że kancelaria zawarła umowę powierzenia jako podmiot przetwarzający. W takiej sytuacji radca ma dalej wszystkie obowiązki opisane w punkcie poprzednim. Godząc się na status podmiotu przetwarzającego w relacji z jednym klientem, radca nie traci statusu administratora w pozostałych relacjach. Dodatkowo:

1) radca już w umowie powierzenia przetwarzania powinien umieścić dane swojego dostawcy email, ze względu na konieczność akceptacji administratora dla dalszych przetwarzających. Zmieniając dostawcę email, radca formalnie powinien wcześniej uzyskać zgodę / brak sprzeciwu takiego klienta (art. 28 ust. 2 RODO).
2) radca powinien zderzyć ze sobą warunki umowy powierzenia z klientem i umowy powierzenia z dostawcą email, aby uniknąć sytuacji sprzeczności tych warunków (art. 28 ust. 4 RODO).

Radca jako podmiot przetwarzający nie mógłby korzystać z dostawcy email, który przechowuje pocztę poza EOG z uwagi na to, że nie istnieją SCC (standardowe klauzule umowne) dla eksporu danych przez podmiot przetwarzający do dalszego podmiotu przetwarzającego[15]. Czyli w naszym przypadku od razu wykluczony byłby iCloud for Business (który i tak wykluczamy ale z innych względów). Praktyczne znaczenie tego problemu formalnego zmalało wskutek wyroku Schrems II, ponieważ transfer „kontentu" do USA obecnie i tak jest bardzo trudny do obronienia prawnie.

Co istotne, należy pamiętać, że w zakresie danych telemetrycznych i danych kontaktowych użytkowników poczty (te które idą do USA nawet gdy kontent pozostaje w UE), administratorem pozostaje sam dostawca email. Dlatego problem braku klauzul SCC przetwarzający do dalszego przetwarzającego nie wystąpi w odniesieniu do dostawców trzymających serwery emailowe w infrastrukturze na terenie EOG.

Warunki świadczenia Usługi email oferowane przez Apple nie zakładają, że Dostawca działa w charakterze dalszego przetwarzającego. Google taką sytuację bierze pod uwagę w swoich dokumentach kontraktowych, podobnie Microsoft. Jeżeli Klient jest podmiotem przetwarzającym wówczas dostawca działa jako podmiot podprzetwarzający.

Na marginesie. Prawna koncepcja ról administrator danych osobowych i podmiot przetwarzający dane, przyjęta w europejskim prawie ochrony danych osobowych, nie jest spójna logicznie. Są argumenty za tym, aby radcę prawnego czy inną organizację korzystającą z usługi poczty elektronicznej uznać za administratora wszystkich danych, z których przetwarzaniem wiąże się wysyłanie poczty, nawet gdy względem tych samych danych taka organizacja jest zasadniczo podmiotem przetwarzającym. Celem niniejszej opinii nie jest jednak rozstrzyganie kwestii akademickich, stąd nie rozwijamy tego wątku.

3. UŚUDE – brak potrzeby regulaminu

UŚUDE. Z art. 8 UŚUDE wynika obowiązek posiadania przez usługodawcę regulaminu usługi świadczonej drogą elektroniczną. W ramach wymiany korespondencji emailowej pomiędzy radcą a jego klientami nie dochodzi jednak w naszej ocenie do świadczenia temu klientowi usługi drogą elektroniczną, dlatego nie ma konieczności sporządzania regulaminu świadczenia usługi drogą elektroniczną.

Jak wynika z powyższego, w zakresie zastosowania UŚUDE ustalenia co do usług email różnią się od naszych ustaleń w opinii wideokonferencyjnej. Różnica polega na tym, że korzystając z usługi

[14] Samych usług email zagadnienie retencji danych dotyczy jednak tylko w niewielkim stopniu, to znaczy należy ustalić, jak długo dostawca emaila przechowuje dane po ich bezpośrednim usunięciu (*soft-deletion*) i po zakończeniu korzystania z usługi, przed ostatecznym usunięciem (*hard-deletion*).
[15] Maciej Gawroński konsultował projekt takich klauzul dla Grupy Roboczej Art. 29 w 2014 roku. Jednak ostatecznie Komisja Europejska skupiła się na przyjęciu RODO w miejsce zatwierdzenia tego typu klauzul.

email nie musimy opracować ani tym bardziej doręczać naszym adresatom ani nadawcom regulaminu naszego emaila.

IV. USŁUGI EMAIL OFEROWANE PRZEZ POSZCZEGÓLNYCH DOSTAWCÓW

1. Microsoft

W zakresie usługi email, jako część pakietu Microsoft 365, Microsoft oferuje:

- **Exchange Online.** Usługa serwera poczty elektronicznej, osadzona w chmurze
- **Outlook online.** Usługa służąca zarządzaniu pocztą elektroniczną użytkownika

2. Google

Oferowany przez Google pakiet G Suite[16] to kompleksowy pakiet usług dla firm Wcześniej usługi te oferowane były pod nazwą Google Apps for Work. Google dzieli usługi G Suite na cztery filary: Komunikacja, Dostęp, Tworzenie i Kontrola.

W zakresie usług email Google oferuje pocztę Gmail. Z pocztą mogą być powiązane inne usługi dostępne w ramach G Suite, z punktu widzenia niniejszej opinii istotne znaczenie ma tu usługa **Cloud Identity Management** – usługa zarządzania i administrowania za pomocą Konsoli Administratora, opisana na stronie: https://cloud.google.com/terms/identity/user-features.html.

Google oferuje różne wersje pakietu usług G Suite: G Suite Basic (wersja, w której użytkownik nie ma możliwości wyboru regionu przetwarzania danych), G Suite Business (wersja najczęściej wybierana, w której możliwy jest wybór regionu przetwarzania danych)[17], G Suite Enterprise, G Suite dla Szkół i Uczelni, Zarchiwizowane konto użytkownika G Suite, G Suite Essentials, G Suite Enterprise Essentials, Cloud Search Platform, Google Voice.

Google od 2012 r. nie oferuje bezpłatnej wersji G Suite[18]. Korzystanie z usługi G Suite niezależnie od wybranego pakietu, rozpoczyna 14 dniowy bezpłatny okres próbny. W procesie rejestracji użytkownik w momencie wyboru nazwy użytkownika i hasła musi zaakceptować warunki Umowy na usługę G Suite – G Suite Agreement oraz **Dodatkowe warunki korzystania z usługi G Suite podczas bezpłatnego okresu próbnego**[19].

3. Apple

Apple dla klientów biznesowych oferuje iCloud Mail w ramach usługi Apple Business Manager. Usługa poczty elektronicznej oferowana jest w ramach zestawu usług oferowanych w pakiecie iCloud. Użytkownicy iCloud, korzystając ze swojego Apple ID mają możliwość utworzenia poczty elektronicznej w domenie @icloud.com[20]. Apple NIE UMOŻLIWIA korzystania z własnej domeny dla celów email[21].

Z usługi iCloud Mail można korzystać z systemu iOS lub macOS czy za pomocą przeglądarki internetowej. Jednak, by utworzyć nowy adres email należy wykorzystać urządzenie wykorzystujące system iOS lub macOS.

Wymagany adres e-mail usługi iCloud Email

Aby korzystać z aplikacji iCloud Mail, utwórz nowy adres e-mail, włączając aplikację Mail w ustawieniach iCloud w systemie iOS lub macOS.

---

[16] https://gsuite.google.com/intl/pl/terms/user_features.html
17 Porównanie wersji G Suite: https://support.google.com/a/answer/6043385
18 Informacje dotyczące wycofanej, bezpłatnej wersji G Suite: https://support.google.com/a/answer/2855120?hl=pl
[19] https://admin.google.com/terms/apps/1/2/pl/supplemental_terms.html
[20] W zależności od tego, kiedy zostało utworzone konto usługi iCloud, adresy email i aliasy usługi iCloud mogą znaleźć się w domenie @icloud.com, @me.com lub @mac.com. (https://support.apple.com/pl-pl/HT201771)
[21] Czytaliśmy o rozwiązaniach hybrydowych polegających na dodatkowym wykorzystaniu usługi podmiotu trzeciego (Fastmail) do połączenia funkcjonalności serwera pocztowego iCloud z adresem we własnej domenie, ale nie jest to przedmiotem opinii.

V. ANALIZA ZGODNOŚCI

Schemat analizy. Analiza zgodności korzystania przed radców prawnych z usług email oferowanych przez Dostawców opiera się na poniższym schemacie:

1) Status dostawcy usługi email

2) Zgodność umowy powierzenia z wymogami art. 28 RODO

3) Legalność transferu danych poza EOG

4) Bezpieczeństwo danych przetwarzanych przez Dostawców [część opisowa]

5) Wiarygodność dostawcy – podsumowanie, informacje o podatnościach, certyfikaty

1. Dostawca usługi email jako przetwarzający i administrator

Do niedawna zgadzano się, że dostawca usługi email działa wyłącznie w roli podmiotu przetwarzającego w rozumieniu art. 4 pkt 8 RODO.

Ostatnio, wskutek analiz spowodowanych wątpliwościami co do usługi Microsoft Office 365, „oficjalnie" spostrzeżono, że w pewnym zakresie dostawca usługi chmurowej działa jako administrator danych osobowych. Chodzi tu o przetwarzanie danych o ruchu i poleceniach w usłudze (dane telemetryczne), dla celów zapewnienia bezpieczeństwa i ciągłości działania, jak i o przetwarzanie danych o konkretnych użytkownikach usługi (login i inne dane uwierzytelniające, dane kontaktowe, imię i nazwisko, inne dane o sobie wprowadzone przez użytkownika – np. zdjęcie).

Spostrzeżenie, że podmiot przetwarzający, szczególnie dostawca usługi chmurowej, może być równolegle administratorem części danych osobowych pozyskiwanych przy świadczeniu usługi, jest prawdziwe nie tylko względem Microsoft, ale i każdego innego dostawcy usługi chmurowej.

1.1. Microsoft

Jak wskazywaliśmy, zasadniczo Microsoft identyfikuje siebie jako podmiot przetwarzający, co odzwierciedla dokumentacja przetwarzania danych osobowych stanowiąca część umów o świadczenie usług oferowanych przez Microsoft. W ograniczonym zakresie, co do przetwarzania niektórych danych (dane telemetryczne i podstawowe dane o użytkowniku), Microsoft „rozpoznał" swoją rolę administratora danych osobowych w nowych dokumentach usługi Microsoft 365[22] ze stycznia 2020. Było to efektem „ostrzału regulacyjnego" ze strony holenderskiego Ministerstwa Sprawiedliwości, Europejskiego Rzecznika Ochrony Danych Osobowych i niemieckich organów ochrony danych osobowych.

1.2. Google

W dokumentacji związanej z usługą G Suite (w tym Gmail), Google identyfikuje się wyłącznie jako podmiot przetwarzający dane na rzecz klienta (użytkownika Usługi G Suite)[23]. Klient biznesowy jest co do zasady administratorem danych Klienta (zgodnie z umową G Suite online – dane przesyłane, przechowywane, wysyłane lub odbierane przy użyciu usług przez Klienta, jego Podmioty stowarzyszone lub użytkowników; dane Klienta obejmują dane osobowe w rozumieniu RODO). Google nie wyklucza także sytuacji, gdy klient będzie podmiotem przetwarzającym (w rozumieniu RODO) dane przetwarzane z wykorzystaniem Gmail. W dokumentacji związanej z usługą G Suite czy Google Cloud, Google nie wskazuje swojej roli jako administratora danych osobowych w odniesieniu do określonych rodzajów danych (np. w odniesieniu do danych telemetrycznych czy zarządzania użytkownikami usług Google).

Google zatem, formalnie nie widzi się w roli administratora danych osobowych świadcząc usługę G Suite dla biznesu. Kwestia roli Google była przedmiotem kontrowersji w odniesieniu międzyinnymi do Google Analytics na etapie przed wejściem w życie RODO, gdy Google wskazał, że uważa się wyłącznie za podmiot przetwarzający dane. „Pozycjonowanie się" Google w tym zakresie jest wiec raczej aktem woli niż niewiedzy.

Jak wskazaliśmy w „opinii wideokonferencyjnej" fakt, że niektórzy dostawcy (tu konkretnie Google) nie rozpoznają swojej roli jako administratora niektórych danych osobowych pozyskiwanych w

[22] Microsoft ostatnio zmienił nazwę swojego pakietu usług z Office 365 na Microsoft 365
[23] art. 5.1 Data Processing Amendment to G Suite and/or Complementary Product Agreement (Version 2.3.) https://gsuite.google.com/terms/dpa_terms.html

związku ze świadczoną usługą chmurową, widząc się jedynie w roli podmiotu przetwarzającego dane powierzone przez klienta, nie wyklucza takiego dostawcy. Jego wiarygodność w tym punkcie jest niższa od wiarygodności dostawcy, który prawidłowo klasyfikuje swoją podwójną rolę. Jednak biznesowy klient danej usługi (w naszym przypadku radca) musi poddać ocenie całokształt okoliczności dotyczących danego dostawcy i usługi przez niego świadczonej, aby ocenić, czy dostawca ten zapewnia „wystarczające gwarancje", o których mowa w art. 28 ust. 1 RODO. Z perspektywy prawnej, dostawca, który całość swojego przetwarzania opiera na powierzeniu danych, znajduje się formalnie w sytuacji lennika swojego klienta, stąd zobowiązuje się wykonywać polecenia klienta także w odniesieniu do danych, którymi realnie administruje.

Również jak wskazaliśmy w opinii konferencyjnej, radca będzie miał obowiązek wskazać podmiotowi danych role, w których występuje dostawca emaila radcy prawnego, oraz zwrócić uwagę na to, że dany podmiot tej konkretnej roli administratora sam nie rozpoznaje, wyjaśniając, że nie powinno to rodzić negatywnych skutków dla tego podmiotu danych i z jakich przyczyn. Wymaga tego, w naszej ocenie, zasada transparentności, o której mowa w art. 5 ust. 1 lit. a RODO[24].

1.3. Apple

W ramach usług oferowanych dla przedsiębiorców Apple wskazuje (w pkt 9 Umowy dotyczącej usług Apple Business Manager (dalej: **Usługa ABM**) https://www.apple.com/legal/enterprise/apple-business-manager/abm-pl.pdf), że Apple w odniesieniu do „kontentu", a więc danych przechowywanych w ramach usług, działa jako podmiot przetwarzający.

Apple w punkcie 10.2 Umowy dotyczącej Usługi ABM wskazuje jednak na dorozumianą zgodę na gromadzenie i przetwarzanie przez Apple danych takich jak unikalne identyfikatory systemowe i sprzętowe, pliki cookies lub adresy IP, informacje o użytkowaniu usługi, ustawieniach rejestracji itp. Dane takie są przetwarzane w celu ułatwienia świadczenia na rzecz użytkowników usług oraz wewnętrznych celów Apple tj. kontrola, analiza danych oraz ulepszenie produktów. Dane dla wyżej wskazanych celów będą przetwarzane zgodnie z polityką prywatności Apple.

Apple przyznaje sobie w istocie także prawo do administrowania wszystkimi danymi powierzonymi dla celów bezpieczeństwa ale i dla egzekwowania umów z Apple (art. 9 ust. 1 zd. 6 Umowy ABM *Apple może ujawnić Dane osobowe o Użytkowniku, jeśli Apple uzna, że ujawnienie jest w uzasadniony sposób niezbędne do egzekwowania warunków i zasad Apple lub zabezpieczania operacji lub użytkowników Apple*).

Apple, w przeciwieństwie do Google, rozpoznaje więc swoją rolę jako administratora niektórych danych osobowych w usługach biznesowych. W tym zakresie idzie jednak bardzo daleko przyznając sobie prawo do ujawniania danych powierzonych w celu wymuszenia warunków umów z Apple[25].

2. Umowa powierzenia

Jednym z głównych obowiązków radców prawnych działających w charakterze administratora danych, w przypadku korzystania z usługi email jest zawarcie umowy powierzenia przetwarzania danych z dostawcą. Wynika to z art. 28 RODO.

Aby ocenić, czy radca prawny w ramach wykonywania zawodu może legalnie korzystać z usługi email oferowanej przez Apple, Google lub Microsoft, w pierwszej kolejności należy ocenić treść zgodności oferowanych umów w zakresie przetwarzania danych osobowych z art. 28 RODO, jak również z innymi obowiązkami wynikającymi z RODO.

2.1. Lokalizacja umów powierzenia

Dostawcy oferują następujące wzorcowe umowy powierzenia przetwarzania danych osobowych:

[24] Oczywiście radca prawny nie ma obowiązku informować o przetwarzaniu danych wielu osób, których dane pozyska pośrednio. Na przeszkodzie stoi tu obowiązek zachowania tajemnicy zawodowej w powiązaniu z wyjątkiem z art. 14 ust. 5 lit. d RODO.

[25] W drodze interpretacji dałoby się to prawdopodobnie w pewnym zakresie pogodzić z RODO (zmiana celu przetwarzania, przetwarzanie w celu dochodzenia, obrony, ustalania roszczeń), ale nie jest naszym zadaniem życzeniowa interpretacja warunków Apple.

2.1.1. **Microsoft**

Zasady powierzenia przetwarzania danych Microsoft przez klient usług online Microsoft opisuje Dodatek dotyczący ochrony danych w ramach usług online Microsoft z 21 lipca 2020 (dalej: **DPA Microsoft**) dostępny pod adresem:

https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=67

2.1.2. **Google**

Korzystając z G Suite klienci w celu spełnienia wymagań RODO powinni zawrzeć z Google:

a) aneks o przetwarzaniu danych – Data Processing Amendment to G Suite and/or Complementary Product Agreement (Version 2.3): https://gsuite.google.com/terms/dpa_terms.html (dalej: **Google DPA**), (który stanowi element Umowy na usługę G Suite- pkt 4.1. G Suite Agreement[26]) oraz uzupełniająco:

b) Standardowe Klauzule Umowne: https://gsuite.google.com/terms/mcc_terms.html (dalej: **Google SCC**)

Radca prawny korzystający z wersji biznesowej Gmaila (w ramach usługi G-Suite) powinien zaakceptować powyższe dokumenty oraz dodatkowo wybrać region, w którym przetwarzane są dane – „Europa". Wybór regionu przechowywania danych możliwy jest tylko w wersjach G Suite Business lub G Suite Enterpise. Zarówno umowy związane z przetwarzaniem danych jak i wybór regionu przetwarzania danych znajdują się w sekcji konsoli administratora Google

G-Suite: KONTO => USTAWIENIA KONTA

Korzystanie z G Suite, niezależnie od wybranego pakietu, rozpoczyna 14 - dniowy bezpłatny okres próbny, do którego zastosowanie mają Dodatkowe warunki korzystania z usługi G Suite podczas bezpłatnego okresu próbnego[27] („**Dodatkowe warunki**"). Zgodnie z pkt 2.6 (Ograniczenia) Dodatkowych warunków:

> *2.6. Niezależnie od jakichkolwiek warunków Umowy G Suite używanie Usług **nie podlega Aneksowi o przetwarzaniu danych**, a Klient zgadza się, że ani on, ani jego Podmioty stowarzyszone i Użytkownicy **nie będą używać Usług do przesyłania, przechowywania, wysyłania ani odbierania jakichkolwiek danych osobowych**.*

Oznacza to, że w trakcie okresu próbnego (bezpłatnego) nie ma zastosowanie Google DPA a użytkownik nie powinien przetwarzać danych osobowych z wykorzystaniem Gmaila. Okres próbny można skrócić, zgodnie z pkt 3.1 Dodatkowych warunków, poprzez kontakt z zespołem pomocy Google i zamianę konta próbnego na standardowe Konto G Suite.

2.1.3. **Apple**

Apple opiera przetwarzanie danych w biznesowej usłudze email:

a) o umowę dotycząca biznesowej wersji usługi iCloud Mail w ramach usługi Apple Business Manager, która w dacie sporządzenia naszej opinii znajdowała się pod następującym adresem https://www.apple.com/legal/enterprise/apple-business-manager/abm-pl.pdf. Zawiera ona w punkcie 9 i częściowo w punkcie 10 postanowienia regulujące dotyczące zasad powierzenia przetwarzania danych osobowych, a dodatkowo

b) o standardowe klauzule umowne, które znaleźliśmy w następującej lokalizacji https://www.apple.com/legal/enterprise/data-transfer-agreements/datatransfer-pl.pdf), oraz

[26] G Suite Agreement dla EEA https://admin.google.com/terms/apps/1/11/en/premier_terms_eea.html
[27] https://admin.google.com/terms/apps/1/2/pl/supplemental_terms.html

c) o zasady ochrony prywatności, które znaleźliśmy pod tym adresem https://www.apple.com/legal/privacy/pl/

Aby korzystać z biznesowej wersji iCloud należy zarejestrować swoją organizację na stronie: https://business.apple.com/#enrollment. Po udanej rejestracji na adres email zgłaszającego zostanie wysłany mail od Apple informujący o zarejestrowaniu zgłoszenia wymagający potwierdzenia zgłoszenia przez wskazaną osobę z organizacji. Po zatwierdzeniu zgłoszenia przez osobę dedykowaną, organizacja będzie musiała zaakceptować warunki i zasady usługi ABM (link przesłany w mailu: https://business.apple.com/#tncs). Na warunki i zasady usługi ABM składają się umowy licencyjne oraz umowa dotycząca usługi ABM, zawierająca regulacje dotyczące zasad powierzenia przetwarzania danych osobowych.

2.2. Zgodność umów powierzenia Dostawców z RODO

Każdy z Dostawców wskazuje swoją rolę jako podmiotu przetwarzającego i zapewnia postanowienia o powierzeniu przetwarzania danych.

Rozliczenie zgodności umów powierzenia z art. 28 RODO. Poniżej przedstawiamy formalne rozliczenie zgodności postanowień wzorcowych umów powierzenia oferowanych przez Dostawców z wymogami RODO w zakresie powierzenia przetwarzania danych.

Tabela 1 – Umowy powierzenia przetwarzania

Lp	Wymóg RODO	Microsoft	Google	Apple
1.	Umowa [RODO 28.3]	DPA Microsoft (uzupełniająco załącznik nr 3 do Dodatku DPA Microsoft)	Aneks o przetwarzaniu danych: Google DPA	Pkt 9. Prywatność i bezpieczeństwo danych umowy ABM – technicznie nie jest to osobny dokument, co utrudnia ocenę zgodności
2.	Dalsze powierzenie [RODO 28.2].	str. 11 Powiadomienie i kontrole dotyczące korzystania z usług Podmiotów Podprzetwarzających, DPA Microsoft Lista dalszych przetwarzających: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2JOJ1	Pkt. 11 Subrocessors Lista dalszych podmiotów przetwarzających, na które ADO wyraża zgodę, oraz ich zadania: https://gsuite.google.com/intl/en/terms/subprocessors.html oraz inne podmioty z grupy Google (nieokreślone)	Pkt 9.1 Używanie i ujawnienie danych osobowych. Lista dalszych podmiotów przetwarzających na żądanie
3.	Zgoda na dalsze powierzenie [RODO 28.2 zd. 2].	str. 11 Powiadomienie i kontrole dotyczące korzystania z usług Podmiotów Podprzetwarzających, DPA Microsoft	pkt. 11.1 Zgoda na podmioty wskazane w powyższym linku. ***Ogólna zgoda na angażowanie nowych podmiotów przetwarzających;*** powiadomienie o nowych przetwarzających.	Pkt 9.1 Używanie i ujawnienie danych osobowych. Lista dalszych podmiotów przetwarzających na żądanie

4.	Sprzeciw względem dalszego powierzenia [RODO 28.2 zd. 2].	str. 11 Powiadomienie i kontrole dotyczące korzystania z usług Podmiotów Podprzetwarzających, DPA Microsoft str. 28 stosowne obowiązki wynikające z RODO	pkt. 11.4 ***Możliwość zgłoszenia sprzeciwu wobec nowego przetwarzającego jedynie poprzez wypowiedzenie umowy G Suite.***	***Brak odpowiednich postanowień wprost.*** *De facto jak w G-Suite sprzeciw tylko przez rezygnację z usługi*
5.	Transfer obowiązków [RODO 28.4].	str. 11, Powiadomienie i kontrole dotyczące korzystania z usług Podmiotów Podprzetwarzających, DPA Microsoft	pkt. 11.3 Requirements for Subprocessor Engagement	Pkt 9.1 Używanie i ujawnienie danych osobowych
6.	Przedmiot przetwarzania [RODO 28.3]	str. 8, Szczegóły dotyczące przetwarzania, DPA Microsoft	Appendix 1: Subject Matter and Details of the Data Processing	***Brak odpowiednich postanowień***
7.	Czas. [RODO 28.3]	str. 8, Szczegóły dotyczące przetwarzania, DPA Microsoft	Appendix 1: Subject Matter and Details of the Data Processing	***Brak odpowiednich postanowień***
8.	Charakter i cel. [RODO 28.3]	str. 8 Szczegóły dotyczące przetwarzania, DPA Microsoft	Appendix 1: Subject Matter and Details of the Data Processing	***Brak odpowiednich postanowień***
9.	Rodzaj danych osobowych. [RODO 28.3]	str. 8, Szczegóły dotyczące przetwarzania, DPA Microsoft str. 5 opis danych przetwarzanych przez Microsoft	Appendix 1: Subject Matter and Details of the Data Processing	***Brak odpowiednich postanowień***
10.	Kategorie osób. [RODO 28.3]	str. 8, Szczegóły dotyczące przetwarzania, DPA Microsoft	Appendix 1: Subject Matter and Details of the Data Processing	***Brak odpowiednich postanowień***
11.	Udokumentowane polecenia [RODO.28.3.a]	str. 8, Role i obowiązki podmiotu przetwarzającego i administratora, DPA Microsoft	Pkt. 5.2.1 Customer's Instructions	Pkt 9.1 Używanie i ujawnienie danych osobowych
12.	Tajemnica [RODO.28.3.b]	str. 11, Zobowiązanie Podmiotu Przetwarzającego do Zachowania Poufności, DPA Microsoft	Pkt.7.1.2 Security Compliance by Google Staff	9.3.1 Procedury bezpieczeństwa; zgodnosc z przepisami Zobowiązanie do przestrzegania obowiązujących

				przepisów dotyczących poufności i bezpieczeństwa – brak zobowiązania do zachowania poufności między stronami umowy.
13.	Przetwarzanie poza EOG [RODO.28.3.a]	str. 10, Lokalizacja i przechowywanie danych, DPA Microsoft	pkt. 10.2 Transfers of Data pkt. 10.3 Data Center Information: lokalizacje centrów danych: https://www.google.com/about/datacenters/locations/index.html	9.4 Dostęp do danych i ich przekazywanie; rozwiązanie Umowy; Instytucja jako Podmiot przetwarzający dane
14.	Bezpieczeństwo. [RODO.28.3.c]	Aneks A — Środki bezpieczeństwa, DPA Microsoft	pkt. 7 Data Security Appendix 2: Security Measures	9.3 Procedury bezpieczeństwa; zgodność z przepisami
15.	Współpraca przy realizacji praw jednostki. [RODO.28.3.e]	str. 8, Prawa osób, których dane dotyczą; pomoc przy wnioskach, DPA Microsoft	pkt. 9.2 Data Subject Requests	Pkt 9.1 Używanie i ujawnienie danych osobowych (wnioski stron trzecich)
16.	Wsparcie przy obowiązkach bezpieczeństwa. [RODO.28.3.f].	str. 28, Stosowne obowiązki wynikające z RODO: art. 28, 32 i 33, DPA Microsoft, Wytyczne przeprowadzania DPiA w Microsoft Office 365[28]	pkt.7.1.3 Additional Security Controls pkt. 7.1.4 Google's Security Assistance pkt. 7.5 Reviews and Audits of Compliance pkt. 8 Impact Assessments and Consultations	9.3 Procedury bezpieczeństwa; zgodność z przepisami
17.	Analiza ryzyka przetwarzania danych osobowych. [RODO 32 RODO]	str. 9, Zasady i procedury bezpieczeństwa, DPA Microsoft	Pkt. 7 Data security Appendix 2: Security Measures	9.3 Procedury bezpieczeństwa; zgodność z przepisami
18.	Powiadomienie o naruszeniu [RODO 33.2]	str. 10, Powiadomienie o Naruszeniu Zabezpieczeń, DPA Microsoft	pkt. 7.2 *brak terminu na powiadomienie administratora o incydencie (określenie: niezwłocznie)*	9.2 Naruszenia bezpieczeństwa danych

[28] https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dpia-office365?view=o365-worldwide#part-2--contents-of-a-dpia

19.	Audyty. [RODO 28.3.h]	str. 9, Kontrola przestrzegania postanowień, DPA Microsoft	pkt. 7.5 Reviews and Audits of Compliance (możliwosc analizy raportów SOC oraz przeprowadzania audytów)	9.3 Procedury bezpieczeństwa; zgodność z przepisami
20.	Współpraca przy audytach [RODO 28.3.h]	str. 9, Kontrola przestrzegania postanowień, DPA Microsoft	pkt. 7.5 Reviews and Audits of Compliance	9.3 Procedury bezpieczeństwa; zgodność z przepisami
21.	Odpowiedzialność za Dalszego Przetwarzającego. [RODO 28.4]	str. 11, Powiadomienie i kontrole dotyczące korzystania z usług Podmiotów Podprzetwarzających, DPA Microsoft	pkt. 11.3.b	***Brak odpowiednich postanowień***
22.	Usunięcie danych osobowych [RODO 28.3.g]	str. 11, Zatrzymywanie i usuwanie danych, DPA Microsoft	pkt. 6.2 Deletion on Term Expiry	9.4 Dostęp do danych i ich przekazywanie; rozwiązanie Umowy; Instytucja jako Podmiot przetwarzający dane
23.	Obowiązek pozostawienia danych osobowych [RODO 28.3.g]	str. 11 Zatrzymywanie i usuwanie danych, DPA Microsoft	pkt. 6.2 Deletion on Term Expiry	9.4.2 Dostęp do danych i ich przekazywanie; rozwiązanie Umowy; Instytucja jako Podmiot Przetwarzający dane

Podsumowanie Tabeli 1

Microsoft. Wzór umowy powierzenia oferowany przez Microsoft adresuje wszystkie wymogi dotyczące takiej umowy wynikające z RODO. Umowa ta jest więc z formalnego punktu widzenia zgodna z prawem i może być zawarta przez radcę prawnego w związku z wykonywaniem przez niego zawodu.

Google. W przypadku angażowania nowych dalszych przetwarzających przez Google, Google umożliwia jedynie rezygnację ze swoich usług jako „sprzeciw" względem zaangażowania konkretnego podwykonawcy. Z uwagi na skalę działalności Google jak i poziom bezpieczeństwa oferowany przez Google (w konsekwencji dobór przez Google jego dostawców), możliwość zgłaszania sprzeciwu wobec nowego podmiotu przetwarzającego jedynie poprzez wypowiedzenie umowy G Suite nie waży negatywnie na wiarygodności Google ani nie stanowi niezgodności z art. 28 ust. 2 RODO.

Google nie wskazuje konkretnego terminu, w ramach którego zmieści się z poinformowaniem klienta o wykrytym naruszeniu ochrony danych, wskazując jedynie, że zrobi to „niezwłocznie". Nie odpowiada to w pełni dosłownej treści art. 33 ust. 1 RODO, która mówi o tym, że termin zgłoszenia naruszenia do organu nadzorczego nie powinien przekroczyć 72 godzin od wykrycia naruszenia. Trudno posądzać Google o nieznajomość RODO, dlatego nie traktujemy tego jako niezgodności z RODO. Pamiętać trzeba też, że interpretacja EROD, jakoby termin 72 godzin biegł od „pierwszego wykrycia naruszenia" (czyli od wykrycia naruszenia przez pierwszy podmiot przetwarzający), jest daleko idąca. Tym niemniej należy obserwować jakie podejście praktyczne Google przyjmie – czy i w jakim terminie będzie informował klientów o naruszeniach, oraz czy ujawnią się okoliczności wskazujące, że Google może zatajać lub opóźniać informacje o naruszeniach ochrony danych.

Podsumowując, umowa powierzenia przetwarzania Google jest w naszej ocenie zgoda z RODO.

Apple. Apple nie oferuje oddzielnej umowy powierzenia przetwarzania danych osobowych, co samo w sobie może być odczytane jako kontrowersyjne na tle wymogu przejrzystości przetwarzania danych z art. 5 ust. 1 lit. a RODO. Postanowienia dotyczące powierzenia przetwarzania danych znajdują się w punkcie 9 i 10 Umowy dotyczącej usługi Apple Business Manager (Umowa ABM).

Umowa ABM nie wskazuje wprost, czego dotyczy powierzenie przetwarzania. Pozostawia to bardzo duże pole do interpretacji, które dane umieszczone na objętych nią urządzeniach Apple są danymi powierzonymi a które prywatnymi (Pkt. 9.1. Umowy ABM mówi tylko o danych osobowych „jeżeli zostaną one dostarczone przez Użytkownika").

Umowa ABM nie zawiera zobowiązania Apple do przedstawiania klientowi zawczasu dalszych podmiotów przetwarzających, co nie jest zgodne z art. 28 ust. 2 zd. 2 RODO.

Nadto Apple przyznaje sobie w istocie prawo do administrowania wszystkimi danymi powierzonymi dla celów bezpieczeństwa ale i dla egzekwowania umów z Apple (art. 9 ust. 1 zd. 6 Umowy ABM *Apple może ujawnić Dane osobowe o Użytkowniku, jeśli Apple uzna, że ujawnienie jest w uzasadniony sposób niezbędne do egzekwowania warunków i zasad Apple lub zabezpieczania operacji lub użytkowników Apple*).

Wszystkie powyższe braki w naszej ocenie nie pozwalają uznać, że Apple oferuje użytkownikom biznesowym zgodną z RODO umowę powierzenia przetwarzania.

3. TRANSFER DANYCH POZA EOG

Wszyscy dostawcy informują, że w ramach korzystania z usług może dochodzić do przetwarzania danych poza EOG tj. poza Europejskim Obszarem Gospodarczym. Przetwarzanie danych osobowych poza EOG wymaga spełnienia dodatkowych warunków określonych w RODO.

3.1. Microsoft

Treści europejskich użytkowników Microsoft 365 domyślnie przechowywane są w europejskich centrach danych Microsoft (Dublin, Amsterdam, Helsinki, Wiedeń, Paryż, Marsylia)[29].

Zgodnie z warunkami świadczenia usług (str. 28 OST Microsoft czerwiec 2020[30]) dane dla: Exchange, Sharepoint i Onedrive domyślnie przetwarzane są w rejonie (*Geo*) lokalizacji klienta Microsoft. Metadane (dane techniczne) jak i dane samych użytkowników (jednolita książka adresowa) przesyłane są do USA.

Microsoft na swoich stronach internetowych[31] pozwala sprawdzić, gdzie przechowywane są dane użytkowników dla usługi Azure Active Directory zapewniającej zarządzanie uwierzytelnianiem użytkowników w usługach Microsoft. Na potrzeby zwykłego uwierzytelnienia dane przetwarzane są wyłącznie w centrach przetwarzania w Amsterdamie lub Dublinie. W przypadku uwierzytelnienia wieloskładnikowego, dane mogą być przetwarzane także w centrach zlokalizowanych w USA.

Transfer danych telemetrycznych i o użytkownikach. Microsoft stosuje w umowach z klientami z UE standardowe klauzule umowne[32]., na podstawie których Microsoft transferuje dane telemetryczne i dane o użytkownikach. Standardowe klauzule umowne stanowią załącznik nr 2 do Dodatku DPA Microsoft. Treść korespondencji email pozostaje (przy zachowaniu ustawień domyślnych usługi) na terenie EOG.

W związku z tym, w naszej ocenie SCC Microsoft stosowane do danych wskazanych w poprzednim zdaniu zapewniają odpowiedni do UE poziom ochrony danych osobowych. Potwierdzają to statystyki

---

[29] https://docs.microsoft.com/pl-pl/office365/enterprise/o365-data-locations?ms.officeurl=datamaps

[30] 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 (email body, calendar entries, and the content of email attachments), (2) SharePoint Online site content and the files stored within that site, and (3) files uploaded to OneDrive for Business.

[31] https://msit.powerbi.com/view?r=eyJrIjoiYzEyZTc5OTgtNTdlZS00ZTVkLWExN2ItOTM0OWU4NjljOGVjIiwidCI6IjcyZjk4OGJmLTg2ZjEtNDFhZi05MWFiLTJkN2NkMDExZGI0NyIsImMiOjV9

[32] https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-eu-model-clauses?view=o365-worldwide

nakazów USA (FISA[33] i NSL[34]), do których odwołuje się NOYB[35], a z których wynika, że ilość żądań niedotyczących kontentu jest pomijalna[36].

Z wyroku Schrems II wynika potrzeba zbadania zagrożenia rządową inwigilacją w USA danych objętych konkretnym transferem. W naszej ocenie w odniesieniu do danych „o użytkowniku" i danych telemetrycznych, standardowe klauzule umowne pozostają skutecznym narzędziem prawnym transferu takich danych osobowych do USA, chroniącym prawa i wolności osób, których transferowane dane dotyczą, w sposób odpowiedni do prawa UE. Wiedza o tym, kto (jaki radca prawny) używa danej usługi email, nie wydaje się mieć bezpośredniego przełożenia na prawa lub wolności klientów czy innych osób, których dane osobowe radca przetwarza (z którymi koresponduje i które są objęte treścią korespondencji). Podobnie informacje o wolumenach przesyłanych danych (ilości emaili radcy i ich rozmiarze ani nawet adresatach – nagłówkach emaili) nie wydają się nawet w szczególnych warunkach mieć wpływu na zagrożenie dla praw lub wolności osób, o których i z którymi radca koresponduje. To wszystko przy założeniu, że treść korespondencji pozostaje na serwerach pocztowych radcy w EOG. W naszej ocenie dostęp rządu USA do danych telemetrycznych i danych o użytkownikach (czyli o radcy i jego współpracownikach) nie zwiększa ryzyka dla praw i wolności osób, z którymi lub o których radca koresponduje, względem ryzyka inherentnie związanego z korzystaniem z poczty elektronicznej jako takiej.

Naszą analizę potwierdzają statystyki żądań ujawnienia danych w trybie Foreign Intelligence Surveillance Act (FISA) i NSL publikowane przez omawianych dostawców, a do których odwołuje się NOYB. Z tych statystyk wynika, że ilość żądań niedotyczących kontentu jest pomijalna[37].

Okoliczność, że Microsoft rozpoznaje swoją rolę jako administratora danych o użytkownikach i danych telemetrycznych nie ma ostatecznie większego wpływu na wynik naszej analizy. Gdyby rola Microsoft w tym zakresie była jednoznaczna, czyli że Microsoft działałby tylko na swoją rzecz, wtedy wręcz można byłoby twierdzić, że co Microsoft robi z takimi danymi, to sprawa Microsoftu a nie radcy. Byłoby to oczywiście rozumowanie instrumentalne. W praktyce jak i formalnie rola Microsoft jest jednak podwójna. Realizuje on zarówno interesy swoje jak i swoich klientów, w tym radcy korzystającego z usługi email. Zatem Microsoft jest w zakresie danych telemetrycznych i danych o użytkownikach równolegle administratorem i podmiotem przetwarzającym. Zagadnienia nie będziemy tu dalej rozwijać, bo jest zbyt akademickie jak na potrzeby przedmiotu opinii

3.2. Google

Zgodnie z pkt 10.1 umowy Google DPA[38], Google może przechowywać i przetwarzać Dane Klienta wszędzie, gdzie Google lub dalsze podmioty przetwarzające mają swoje lokalizacje, z zastrzeżeniem, że Google:

a) zapewni odpowiednią podstawę prawną transferu danych poza EOG (standardowe klauzule umowne zwane przez Google *Model Contract Clause*s lub Alternatywna Podstawa Transferu –*Alternative Transfer Solution*)

b) uwzględni mające zastosowanie Szczegółowe warunku korzystania z usługi G Suite w zakresie lokalizacji danych.

Zgodnie z pkt. 1.1. Szczegółowych warunków korzystania z usługi G Suite[39], klient może skorzystać z tzw. Konsoli Administracyjnej, **aby wybrać Region danych** (tj. USA lub Europę) do przechowywania w spoczynku Danych zlokalizowanych. „Dane zlokalizowane" to dane główne wchodzące w skład Danych Klienta z odpowiedniej usługi. W zakresie usługi email – Gmail są to: temat, treść emaila, załączniki oraz adresy nadawców i odbiorców wiadomości.

W umowie Google DPA Google wskazuje również lokalizacje centrów przetwarzania danych, które dostępne są na stronie internetowej:

[33] Foreign Intelligence Security Act
[34] National Security Letters
[35] https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report, https://transparencyreport.google.com/user-data/us-national-security?hl=pl, https://www.apple.com/legal/transparency/pdf/requests-2019-H1-en.pdf
[36] https://noyb.eu/en/next-steps-eu-companies-faqs
[37] https://noyb.eu/en/next-steps-eu-companies-faqs
[38] https://gsuite.google.com/terms/dpa_terms.html
[39] https://gsuite.google.com/terms/service-terms/

https://www.google.com/about/datacenters/locations/index.html.

W Europie Google przetwarza dane w następujących centrach przetwarzania danych:

a) Dublin, Ireland

b) Eemshaven, Netherlands

c) Fredericia, Denmark

d) Hamina, Finland

e) St. Ghislain, Belgium

Podobnie jak w przypadku Microsoft i z tych samych powodów oceniamy, że SCC Google zapewniają odpowiedni do UE stopień ochrony danych osobowych dla innych danych niż „Dane zlokalizowane" w rozumieniu wyżej wskazanym.

3.3. Apple

Apple nie określa precyzyjnie, w jakich lokalizacjach przetwarza dane osobowe. Apple wskazuje (pkt 9.3 Umowa dotycząca Usługi ABM), że zaszyfrowane dane osobowe mogą być przechowywane w lokalizacji znanej tylko Apple. Dodatkowo Apple w oświadczeniu „Omówienie kwestii bezpieczeństwa w usłudze iCloud"[40] wskazuje, że niektóre dane przechowywane w iCloud mogą być przetwarzane w serwerach należących do partnerów zewnętrznych tj. Amazon Web Services lub Google Cloud Platform.

W konsekwencji **podstawowe i kontaktowe dane użytkownika**: oraz treść maili/ kontent mogą być (i zapewne są) transferowane poza EOG czy to w ramach grupy Apple czy w ramach korzystania z podwykonawców.

SCC Apple. W odniesieniu do użytkowników z Europejskiego Obszaru Gospodarczego, spółką, która zawiera umowę z użytkownikiem biznesowym, jest Apple Distribution International Ltd. z siedzibą w Irlandii.

Zgodnie z pkt. 9.4. Umowy dotyczącej Usługi ABM, dane w ramach świadczenia usług przez Apple mogą być transferowane do tzw. państw trzecich. Apple z siedzibą w Irlandii jako administrator danych w ramach świadczenia usług może przekazywać dane do Apple w Stanach Zjednoczonych na podstawie standardowych klauzul umownych (https://www.apple.com/legal/enterprise/data-transfer-agreements/datatransfer-pl.pdf). Zapewne to Apple z siedzibą w Stanach Zjednoczonych korzysta z usług dalszych przetwarzających tj. Google czy AWS.

Zgodnie z dodatkiem nr 1 do SCC zakres danych transferowany do Stanów Zjednoczonych obejmuje w zasadzie wszystkie informacje o użytkowniku, jakie zbiera Apple z siedzibą w Irlandii.

W praktyce radcowie, którzy zdecydują się na konfigurację swojej poczty elektronicznej z iCloud'em, nie będą mogli mieć wpływu na miejsce przechowywania treści ich maili czy załączników przesyłanych w mailach. Na tle wyroku Schrems II oznacza to w naszej ocenie, że o ile radca nie zastosuje rozwiązania technicznego szyfrującego treść emaila, to istnieje wysokie ryzyko, iż klauzule SCC oferowane przez Apple nie zapewnią odpowiedniego stopnia ochrony danych osobowych pozwalającego na korzystanie przez radcę prawnego z poczty iCloud dla celów służbowych. Zachodzić będzie bowiem sytuacja wprost opisana w wyroku Schrems II – kompletne dane usługi email będą znajdować się w USA i rząd USA będzie mógł nakazać Apple ich ujawnienie.

Widzimy pewne argumenty za tym, aby w konkretnych sytuacjach uznać SCC Apple za wystarczające do zapewnienia odpowiedniego stopnia ochrony danych osobowych znajdujących się w korespondencji wykorzystującej usługę iCloud Mail:

- Analiza raportu Apple na temat rządowych żądań ujawnienia danych za 1-6.2019 wskazuje na relatywnie niską ilość żądań dostępu rządu USA i niższą ilość udostępnionych danych (dane z ok 4 tys urządzeń udostępniono przy żądaniach dotyczących ponad 11 tys urządzeń). Apple jest znane z dbałości o prywatność użytkowników.

[40] https://support.apple.com/pl-pl/HT202303

- Radca, decydując się na korzystanie z poczty iCloud, powinien ostrzegać klienta w umowie lub pierwszej komunikacji, że jeżeli klient lub osoby, których dotyczy korespondencja, może lub mogą być w orbicie zainteresowania USA, inny dostawca komunikacji powinien być stosowany.
- Alternatywnie radca może zastosować wyższy standard ochrony poczty email niż standard IMAP. Zastosowanie takiego wyższego standardu ochrony (S/MIME lub PGP) wymaga jednak zachodu zarówno po stronie radcy jak i odbiorców jego emalii i nie jest popularne.
- Alternatywnie radca dla szczególnie wrażliwej korespondencji powinien stosować inny kanał komunikacji niż email, na przykład wiarygodny szyfrowany komunikator z możliwością ustawiania wygasania wiadomości, lub wręcz komunikację bezpośrednią, jeśli to możliwe.
- Alternatywnie, radca może uznać, że prowadzi na tyle lokalną praktykę, że USA jego klientami na pewno nie będzie się interesować.

W każdym przypadku jednak radca chcąc skorzystać z iCloud Mail dla celów służbowych musiałby sporządzić dodatkową ocenę ryzyka dla celów potwierdzenia adekwatności ochrony danych w ramach iCloud Mail. Nie mógłby oprzeć się wyłącznie na naszej opinii, której generalne wnioski są dla iCloud Mail niekorzystne. Pamiętać też trzeba o wyżej wskazanych przez nas wątpliwościach co do zgodności z RODO samych warunków przetwarzania danych oferowanych przez Apple.

3.4. Szyfrowanie danych w tranzycie

Jak wskazujemy w dalszej części opinii, wszyscy dostawcy zapewniają kryptograficzną ochronę danych w przesyle z pomocą protokołu TLS. Stwierdzenie to jest istotne dla wyników analizy, ponieważ TSUE wskazał też na możliwość „podsłuchu" danych wysyłanych do USA kablem transatlantyckim.

4. BEZPIECZEŃSTWO DANYCH

4.1. 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. 35 RODO

*1. Jeżeli dany rodzaj przetwarzania – w szczególności **z użyciem nowych technologii** – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.*

3. Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:

a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10; lub

c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

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.

4.2. Stan wiedzy technicznej, środki bezpieczeństwa i cel ich stosowania

W oparciu o art. 32 RODO, każdy administrator danych ma obowiązek przeprowadzenia analizy ryzyka w celu określenia czy środki organizacyjne i techniczne jakie stosuje wobec przetwarzania danych (on sam lub podmiot przetwarzających) są odpowiednie do ryzyka naruszenia praw lub wolności osób, których dane dotyczą. Radcy prawni z uwagi na obowiązującą ich tajemnicę zawodową powinni dołożyć szczególnej staranności w celu zapewnienia przetwarzanym danym odpowiedniego poziomu bezpieczeństwa.

Ustalając, czy usługi 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 [41] . Wyczerpujący i aktualny na datę sporządzenia zestaw środków zabezpieczenia danych został opisany przez niemiecką agencję Teletrust[42] we współpracy z ENISA[43]

[41] norma ISO/IEC 27001:2017, NIST Special Publication 800-53 https://nvd.nist.gov/800-53
[42] https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/
[43] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

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.

4.3. Podstawowe środki bezpieczeństwa

RODO nie wskazuje konkretnych środków bezpieczeństwa, podając jako przykładowe tylko niektóre z możliwych (np. szyfrowanie i pseudonimizację, regularne testowanie). Biorąc pod uwagę sposób oraz kontekst planowanego wykorzystania usług przez radców, na podstawie powyżej wskazanych źródeł można odtworzyć listę podstawowych środków bezpieczeństwa, jakie usługi powinny zapewniać. Chodzi tu o wewnętrzne, niejako wbudowane bezpieczeństwo usługi, ale także o funkcjonalności, które pozwolą klientowi zarządzać bezpieczeństwem danych przetwarzanych w usłudze w ramach własnego systemu zarządzania bezpieczeństwem informacji - np. możliwość zarządzania dostępami i uprawnieniami użytkowników swojej organizacji. Dla przejrzystości, przy każdym ze środków podajemy odniesienie do odpowiednich postanowień normy PN-EN ISO/IEC 27001:2017-06.

1. Zabezpieczenie przesyłanych i przechowywanych danych, w tym szyfrowanie (A.10.1, A 13.2)
2. Zabezpieczenia przed złośliwym oprogramowaniem (A.12.2)
3. Uwierzytelnianie użytkowników (A.9.4.1, A.9.4.2.)
4. Zarządzanie dostępami i uprawnieniami użytkowników oraz administratorów (A.9.1.1., A.9.2.)
5. Ciągłość i dostępność usługi (A.17.1, A 17.2)
6. Tworzenie kopii zapasowych informacji (A.12.3.1)

4.4. Cel stosowania środków bezpieczeństwa

Stosowanie środków bezpieczeństwa zapewnić ma bezpieczeństwo informacji. Najczęściej bezpieczeństwo informacji definiowane jest poprzez triadę z angielskiego określaną skrótem *CIA*, pod którym kryją się jego następujące atrybuty – poufność (*confidentiality*), integralność (*integrity*), dostępność (*availability*). Definicje tych atrybutów zawiera norma ISO 27000:2018:

Poufność – zapewnienie, że informacja nie jest dostępna lub ujawniona nieuprawnionym osobom, podmiotom lub procesom (3.10)

Integralność – dokładność i kompletność informacji (3.36)

Dostępność – zapewnienie, że informacja jest dostępna i nadająca się do użytku przez uprawnione podmioty (3.7)

Zgodnie z art. 5 ust. 1 lit. f RODO obowiązek zapewnienia integralności i poufności danych osobowych stanowi jedną z podstawowych zasad przetwarzania danych osobowych przez administratora:

> *art. 5 ust. 1. lit. f 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").*

4.5. Środki bezpieczeństwa

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.

Co istotne, poziom zapewnianych środków bezpieczeństwa zależy od wariantu usługi, z którego korzysta użytkownik. Poniżej opisujemy podstawowe środki zapewniane przez Dostawców w ramach omawianych usług. Każdorazowo zalecamy jednak szczegółową weryfikację wersji planu o zastosowanej konfiguracji, z której radca korzysta, w celu potwierdzenia środków bezpieczeństwa stosowanych i udostępnianych w usłudze.

Jako plan minimum bezpiecznego korzystania z usługi **rekomendujemy**:

1. wyznaczenie użytkownika lub użytkowników pełniących rolę administratora przy jednoczesnym ograniczeniu zakresu uprawnień pozostałych użytkowników,
2. bieżące zarządzanie dostępami użytkowników – w szczególności niezwłoczne usuwanie dostępów i uprawnień użytkowników, w przypadku ich odejścia z organizacji,
3. weryfikację domyślnych ustawień szyfrowania w usłudze i uaktywnienie właściwych funkcji w tym zakresie,
4. weryfikację domyślnych ustawień w zakresie skanowania *anti-malware* poczty i uruchomienie tej funkcji,
5. samodzielne wykonywanie kopii danych istotnych przechowywanych w usłudze i przechowywanie ich w innej lokalizacji niż usługa poczty, jeżeli usługa nie zapewnia mechanizmów automatycznego tworzenia kopii zapasowych (z tym że w mniejszych organizacjach urządzenia użytkowników można uznać w naszej ocenie za backup rozproszony poczty elektronicznej).

4.6. Szyfrowanie danych – przesyłanych i przechowywanych

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* = szyfrowanie danych w spoczynku).

W praktyce niewykonalne natomiast jest otwieranie plików przez aplikacje bez odszyfrowywania plików (np. praca na dokumencie Word wymaga odszyfrowania pliku tekstowego, np. docx, .rtf)[44].

W przypadku szyfrowania danych w przesyle istotne jest, pomiędzy którymi dwoma punktami przesyła się informacje zaszyfrowane. Szyfrowanie na pełnej drodze między urządzeniem, w którym nadawca wprowadza komunikat, a urządzeniem, na którym odbiorca odczytuje komunikat, nazywamy szyfrowaniem *end-to-end*.

Równie istotne jest tutaj zagadnienie szyfrowania danych *at rest* – maili, treści, danych przechowywanych na serwerze poczty, dysku wirtualnym, dysku wspólnym lub w ramach innych usług chmurowych. Zasadniczo istnieją trzy stany: (i) dane nieszyfrowane w spoczynku, (ii) dane szyfrowane w spoczynku ale klucze szyfrujące posiada dostawca usługi przechowywania, (iii) dane zaszyfrowane w spoczynku, których hostingodawca nie może rozszyfrować.

Serwery pocztowe. Serwery poczty wychodzącej (obecnie stosujące protokół *SMTP* w miejsce starszego *POP3*) obsługują wysyłanie wiadomości. Serwery poczty przychodzącej odpowiadają za wiadomości przychodzące. Na kontach IMAP, w przeciwieństwie do POP3, kopie wiadomości są przechowywane na serwerze poczty przychodzącej, dopóki nie zostaną osobno usunięte. Pozwala to synchronizować pocztę na wielu urządzeniach końcowych.

4.6.1. **Microsoft**

Rozwiązania technologiczne usług pakietu Microsoft 365 zapewniają szyfrowanie danych zarówno *at rest* jak *in transit* za pomocą różnych technologii w zależności od rodzaju danych i usługi[45]. Rozwiązania standardowo proponowane przez Microsoft nie zapewniają szyfrowania *end-to-end*.

Szyfrowanie *at rest*. Dane znajdują się w stanie *at rest* (czyli w spoczynku), m.in. gdy są przechowywane w skrzynce mailowej w ramach usługi *Exchange Online*. Szyfrowanie dotyczy zarówno treści wiadomości jak i załączników. Centra przetwarzania danych Microsoft wykorzystywane do świadczenia usług w ramach Microsoft 365 wykorzystują technologię BitLocker (opartą m.in. na szyfrowaniu AES standardem 256-bitowym) oraz Distributed Key Manager.

Szyfrowanie *in transit*. Dane znajdują się w przesyle – *in transit*, za każdym razem, gdy dochodzi do komunikacji urządzeń użytkownika z serwerami Microsoft lub gdy serwer Microsoft komunikuje się z innymi serwerami. Dotyczy to zatem przykładowo sytuacji, gdy użytkownik uzyskuje dostęp do danych przechowywanych w usłudze Echange Online lub wysyła wiadomości mailowe. Podstawową

[44] 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.

[45] https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption?view=o365-worldwide

technologią kryptograficzną wykorzystywaną do ochrony tych danych *in transit* jest TLS (*Transport Layer Security*) w wersji 1.2. W przypadku wiadomości mailowych Microsoft zapewnia także dodatkowe, opcjonalne narzędzia [46]. Należy do nich Office 365 Message Encryption (OME) pozwalający wysyłać zaszyfrowane wiadomości email. Dla odbiorców korzystających z Outlooka, użycie OME nie wpływa na sposób odbioru i odczytania wiadomości. Dla użytkowników innych klientów poczty, może oznaczać konieczność wyświetlenia wiadomość poprzez OME Portal. Innym rozwiązaniem jest technologia S/MIME pozwalająca cyfrowo podpisywać i szyfrować wiadomości.

Azure Information Protection i Azure Rights Management. Usługi Azure Information Protection i Azure Rights Management pozwalają klientowi zarządzać bezpieczeństwem informacji. Oferują one narzędzia pozwalające m.in. oznaczać wrażliwość dokumentów, automatycznie stosować dla nich zabezpieczenia takie jak ograniczenia możliwości skopiowania, zmiany, czy wysyłki, udostępnienie wyłącznie wybranym grupom użytkowników, czy szyfrowanie, na podstawie ustalonych przez użytkownika – administratora reguł i polityk.

Data loss prevention. Usługi Microsoft 365 oferują możliwość wdrożenia przez klienta usługi - administratora – polityki typu *data loss prevention*. Narzędzie to pozwala automatycznie identyfikować wrażliwie informacje i zapobiegać ich ujawnieniu, np. poprzez blokowanie możliwości wysłania wiadomości email taką informację zawierającą. Usługa automatycznie rozpoznaje określone kategorie danych, chociażby numery kart kredytowych, zapobiegając ich wyciekowi.

Zaznaczamy, że w praktyce funkcjonowania niedużej kancelarii prawnej korzystanie z funkcjonalności ustawiania reguł i polityk typu DLP czy klasyfikowania wrażliwości informacji wydaje się niełatwe.

4.6.2. **Google**

Jak wynika z szeregu deklaracji Google oraz z umowy Google DPA, podobnie jak Microsoft, Google stosuje szyfrowanie danych w tranzycie (*in transit*) i w spoczynku (*at rest*)[47]. Google w deklaracji dostosowania do RODO (General Data Protecion Regulation – Google Cloud Whitepaper z maja 2018 r.) wskazuje szyfrowanie jako jeden z podstawowych środków bezpieczeństwa stosowanych przez Google, zarówno wobec danych przesyłanych w Internecie, pomiędzy centrami danych Google jak i przechowywanych przez Google.

Szyfrowanie „in transit". Google stosuje szyfrowanie danych w transmisji siecią Internet jak i siecią Google (gdy dane przesyłane są pomiędzy centrami danych Google). Google szyfruje dane w transmisji zarówno pomiędzy użytkownikiem a Google jak i pomiędzy użytkownikiem Google a podmiotem trzecim.

Transmisja danych pomiędzy użytkownikiem usługi G Suite a Google jest chroniona za pomocą szyfrowania w sposób automatyczny. Google stosuje protokół TLS (Transport Layer Security)[48]. Zapobiega to przechwytywaniu i zmienianiu przesyłanych danych, niezależnie od tego czy użytkownik korzysta z publicznego WiFi, biurowej sieci czy pracuje z domu. Google szyfruje dane w tranzycie z użyciem sprawdzonych algorytmów szyfrujących: RSA oraz ECDSA. Należy pamiętać, że protokół TLS może być stosowany na całej drodze wiadomości email, tylko o ile serwer i urządzenie odbiorcy obsługują standard TLS.

Opcjonalnie, Google oferuje zaawansowany standard szyfrowania - hostowane szyfrowanie w standardzie S/MIME (Secure/Multipurpose Internet Mail Extensions)[49]. Funkcja ta jest dostępna dla wersji G Suite Enterprise (a więc najbardziej „zaawansowanej"). Aby szyfrowanie S/MIME działało, musi być włączone zarówno u nadawcy jak i adresata.

Szyfrowanie „at rest". Szyfrowanie danych w spoczynku stosowane jest wobec danych przechowywanych przez Google na dyskach oraz na kopiach zapasowych. Szyfrowanie danych „at rest" zapewnia ochronę, nawet w sytuacji, gdy ktoś przełamie zabezpieczenia fizyczne i uzyska

[46] https://docs.microsoft.com/en-us/microsoft-365/compliance/email-encryption?view=o365-worldwide
[47] https://cloud.google.com/security/gdpr/resource-center/pdf/googlecloud_gdpr_whitepaper_618.pdf
[48] https://gsuite.google.com/terms/dpa_terms.html
[49] https://support.google.com/a/answer/7280976?hl=pl&ref_topic=9061730

dostęp fizyczny do sprzętu, na którym przechowywane są dane. Szyfrowanie chroni dane w ten sposób, że osoba przełamująca zabezpieczenia fizyczne nie będzie w stanie odczytać danych.

Google szyfruje dane „at rest" automatycznie, bez jakichkolwiek działań czy inicjatyw użytkownika usług. Google szyfrując dane „at rest" dzieli dane przesłane przez użytkowników na podpliki – tzw. fragmenty albo porcje (ang. „*chunks*") i przechowuje te fragmenty plików (danych) pod unikalnym ID dla każdego fragmentu. Każdy fragment ma przypisywany swój klucz powiązany z określoną Listą Kontrolą Dostępu (Access Control List (ACL). ACL zapewnia, że każdy fragment może być odszyfrowany przez upoważnionego pracownika Google i określone w momencie szyfrowania danych usługi. W konsekwencji, każdy fragment jest zaszyfrowany za pomocą innego klucza szyfrującego, nawet jeżeli dane należą do tego samego użytkownika. Fragmenty zaszyfrowane są za pomocą 128 lub 256-bitowego klucza AES – Advanced Encryption Standard[50]. Dane szyfrowane przez Google w sposób opisany powyżej to tzw. „Core Content", który obejmuje w zakresie Gmail wiadomości i załączniki.

Stosowany do szyfrowania danych w spoczynku przez Google Zaawansowany Standard Szyfrowania – AES, pierwotnie nazywany Rijndael, **jest jedną z najczęstszych metod szyfrowania ważnych danych**, używaną przez organizacje od Apple i Microsoft po NSA (amerykańską *National Security Agency*).

4.6.3. **Apple**

Szyfrowanie maili ogólnie. Apple jako jeden z gigantów technologicznych promuje podejście oparte o prywatność danych swoich użytkowników i zapewnia szereg funkcjonalności umożliwiających zapewnienie bezpieczeństwa przesyłanych i przechowywanych danych.

Szyfrowanie w przesyle. Cały ruch między urządzeniami a usługą iCloud Mail jest szyfrowany przy użyciu standardu TLS 1.2. (szyfrowanie *in transit*). Nie oznacza to jednak, że wiadomości email będą zawsze wysyłane w formacie TLS. Domyślnie serwery pocztowe od dużych dostawców wysyłają wiadomości w formacie TLS do tych odbiorców, którzy ten format obsługują. Zatem serwer odbiorcy poczty też musi obsługiwać TLS.

Standardowo usługa iCloud korzysta z serwerów poczty IMAP, co oznacza, że treść emaili na serwerze pocztowym nie jest zabezpieczona szyfrowaniem przed dostępem samego dostawcy poczty (czyli Apple). Wszystkie programy pocztowe Apple obsługują (opcjonalne) szyfrowanie S/MIME (Secure/Multipurpose Internet Mail Extensions)[51].

S/MIME dla pojedynczych wiadomości. Apple obsługuje standard S/MIME dla pojedynczych wiadomości. Oznacza to, że użytkownicy korzystający z S/MIME mogą wybrać domyślne podpisywanie i szyfrowanie wszystkich wiadomości lub podpisywać i szyfrować pojedyncze wiadomości.

Tożsamości używane przez standard S/MIME mogą być dostarczane do urządzeń Apple przy użyciu usług zewnętrznych dostawców tożsamości, w tym w szczególności Microsoft Active Directory.

W praktyce, jeżeli radca chciałby zapewnić pełne szyfrowanie emaili pomiędzy sobą a odbiorcą (*end-to-end encryption*), obie strony muszą dysponować stosownymi certyfikatami i dodatkowym oprogramowaniem. Sam fakt korzystania z iCloud nie zapewnia tego standardu. Ma to znaczenie dla oceny legalności korzystania z iCloud na tle Schrems II.

Jak wskazaliśmy wyżej, w rozdziale o transferze danych do USA, na tle wyroku Schrems II trudno uznać SCC Apple za ogólnie skuteczne w odniesieniu do korzystania z serwerów email usługi iCloud znajdujących się w USA. Korzystanie z usługi iCloud dla celów profesjonalnych przez radców prawnych po wyroku Schrems II można byłoby próbować uznać za legalne pod kilkoma warunkami:

- Apple nie umożliwia ograniczenia przechowywania danych w Europejskim Obszarze Gospodarczym, a w konsekwencji dane te wprost podlegają pod nakazy FISA.
- Jednak analiza raportu Apple na temat rządowych żądań ujawnienia danych za 1-6.2019 wskazuje na relatywnie niską ilość żądań dostępu rządu USA i niższą ilość udostępnionych danych (dane z ok 4 tys urządzeń udostępniono przy żądaniach

[50] https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf str. 3
[51] https://support.apple.com/pl-pl/HT202303

dotyczących ponad 11 tys urządzeń). Apple jest znane z dbałości o prywatność użytkowników.

- W związku z tym radca, decydując się na korzystanie z poczty iCloud, mógłby ostrzegać klienta w umowie lub pierwszej komunikacji, że jeżeli klient lub osoby, których sprawa dotyczy, mogą być w orbicie zainteresowania USA, inny dostawca komunikacji powinien być stosowany. Alternatywnie
- radca mółby zastosować wyższy standard ochrony poczty email niż standard IMAP. Zastosowanie takiego wyższego standardu ochrony (S/MIME lub PGP) wymaga jednak zachodu zarówno po stronie radcy jak i odbiorców jego emaili i nie jest popularne. Alternatywnie
- radca dla szczególnie wrażliwej korespondencji mógłby stosować inny kanał komunikacji niż email, na przykład wiarygodny szyfrowany komunikator z możliwością ustawiania wygasania wiadomości (co i tak jest zalecane dla komunikacji, którą mogłyby być zainteresowane nasze rodzime służby).

Szyfrowanie at rest. Tak jak zostało wspomniane powyżej, maile hostowane w iCloud at rest (w spoczynku) nie są szyfrowane.

Data	Encryption	
	In transit	On server
Mail	Yes	No

Źródło: *Omówienie kwestii bezpieczeństwa w usłudze iCloud (dostęp 17.08.2020)*[52].

4.7. Zabezpieczenia przed złośliwym oprogramowaniem

Użytkownik – radca prawny może i powinien samodzielnie zabezpieczać urządzenia, z których korzysta, przed złośliwym oprogramowaniem (malware). Malware stanowi dziś podstawowe zagrożenie dla poufności, integralności i dostępności informacji użytkownika. Do ochrony służy między innymi oprogramowanie antywirusowe. Standardem są dziś jednak także wbudowane rozwiązania zapewniane przez same usługi, np. automatycznego skanowania poczty elektronicznej, pozwalające skutecznie chronić przed malware. Takie wbudowane rozwiązania zapewnia w ramach rozważanych tu usług każdy z dostawców.

4.7.1. **Microsoft**

Podstawowym narzędziem typu anti-malware zapewniającym bezpieczeństwo w usługach poczty Exchange Online jest usługa Exchange Online Protection (EOP)[53]. Jej uruchomienie nie wymaga dodatkowych działań po stronie użytkownika, jest ona wbudowana w usługę Exchange Online i domyślnie włączona (działa *by default*). EOP zapewnia skanowanie wiadomości mailowych transportowanych w ramach usługi Exchange Online. W razie wykrycia malware wiadomości poddawane są kwarantannie lub usuwane. Klient usługi ma możliwość skonfigurowania własnych anti-malware'owych polityk w ramach usługi obejmującej np. możliwość zablokowania w ogóle możliwości odbioru wiadomości zawierających załączniki o określonym rozszerzeniu (np. .exe lub .jar). Skanowanie anti-malware w ramach EOP dotyczy nie tylko przesyłanych wiadomości, ale obejmuje również skanowanie retroaktywne wiadomości już przechowywanych w skrzynce, poprzez usługę Zero-hour Auto Purge (ZAP)[54]

W pewnym zakresie Microsoft zapewnia ochronę przed atakami typu ransomware, jeżeli tego rodzaju atak dotknąłby skrzynkę mailową. Usługa oparta jest na funkcjonalnościach związanych z

[52] https://support.apple.com/pl-pl/HT202303
[53] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide
[54] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/virus-detection-in-spo?view=o365-worldwide

tzw. *soft* and *hard deletion*, zgodnie z którymi usunięte ze skrzynki wiadomości lub nawet całą skrzynkę można przywrócić przed upływem określonego czasu od tego usunięcia – zasadniczo 30 dni. Więcej na temat tej funkcjonalności piszemy w dalszej części poświęconej kopiom zapasowym.

Użyliśmy pojęcia ochrony „w pewnym zakresie", gdyż Microsoft wskazuje, że w przypadku rzadkiej sytuacji, gdy ransomware usunie wszystkie emaile, „you can probably recover the deleted items"[55]. Efekt „anty-maleware" opóźnienia trwałego usunięcia emaili jest raczej wynikiem tej funkcjonalności niż jej pierwotnym celem oraz nie zawsze zadziała (przejęcie uprawnień administratora usługi Microsoft 365 przez złośliwe oprogramowanie mogłoby zapewne doprowadzić także do trwałego usunięcia zawartości serwerów email, gdyby tak **skonstruować** złośliwe oprogramowanie lub gdyby był to atak sterowany manualnie).

4.7.2. **Google**

Zabezpieczenia przed złośliwym oprogramowaniem stanowi część bezpieczeństwa operacyjnego deklarowanego przez Google (zgodnie z dokumentem Google Cloud Security and Compliance How Google protects your data)[56]. We wskazanym w zdaniu poprzednim dokumencie Google deklaruje, że jego

strategia dotycząca złośliwego oprogramowania (strategia anit-malware) opiera się na zapobieganiu infekcjom poprzez użycie ręcznych i automatycznych skanerów do przeszukiwania indeksu wyszukiwania Google w poszukiwaniu witryn, które mogą być niebezpieczne pod kątem złośliwego oprogramowania lub phishingu.

W ramach Gmail, Google skanuje wszystkie wiadomości w celu ochrony przed złośliwym oprogramowaniem, niezależnie od tego, czy zaawansowane ustawienia zabezpieczeń załączników są włączone czy nie[57]. Google oferuje użytkownikom G Suite dodatkowe zabezpieczenia przed złośliwym oprogramowaniem, które są zalecane w szczególności dla nowych użytkowników (z krótką historią mailową w Gmail). Aby uruchomić bardziej zaawansowane niż standardowe zabezpieczenia przed złośliwym oprogramowaniem, po zalogowaniu do konta użytkownika (poprzez: https://admin.google.com), użytkownik musi za pomocą konsoli administracyjnej wybrać opcje: APLIKACJE => G Suite => GMAIL => **BEZPIECZEŃSTWO**.

W sekcji „Bezpieczeństwo" dla Gmail, użytkownik może zarządzać ustawieniami zabezpieczeń dla:

a) **Załączników –** w tym zakresie **domyślnie włączone są:**

- Ochrona przed zaszyfrowanymi załącznikami od niezaufanych nadawców
- Ochrona przed załącznikami zawierającymi skrypty od niezaufanych nadawców

Możliwe do wyboru przez użytkownika – Administratora G Suite działania związane z e-mailami zawierającymi wyżej wskazane załączniki (tj. od niezaufanych nadawców lub zawierające skrypty od niezaufanych nadawców) to a) zachowanie wiadomości e-mail Odebranych i ostrzeżenie (ustawione przez Google domyślnie), b) przeniesienie wiadomości e-mail do spamu lub c) kwarantanna.

Google zapewnia również możliwość zmiany ustawień w zakresie Ochrony przed nietypowymi załącznikami do e-maili, dając użytkownikowi możliwość wyboru takich samych działań jak w przypadku e-maili z załącznikami od niezaufanych nadawców. Użytkownik ma również możliwość dodania niektórych rzadkich typów plików do białej listy.

b) **Linków i obrazów zewnętrznych –** w zakresie bezpieczeństwa linków i obrazów przesyłanych poprzez Gmail, Google zapewnia:

- Identyfikacje linków w skróconych adresach URL (co umożliwia wykrywanie złośliwych linków ukrytych w skróconych adresach URL) – domyślnie włączone,
- Skanowanie obrazów, do których prowadzą linki - domyślnie włączone,

[55] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/recover-from-ransomware?view=o365-worldwide
[56] https://gsuite.google.com/learn-more/security/security-whitepaper/page-3.html
[57] G Suite Admin help: Advanced phishing and anti-malware protection: https://support.google.com/a/answer/9157861?hl=en

- Ostrzeżenia, jeśli kliknięty link prowadzi do niezaufanej domeny- domyślnie włączone.

c) Podszywania się i uwierzytelniania – w tym zakresie Google zapewnia:

- Ochronę przed wiadomościami pochodzącymi z domen, których nazwy wizualnie przypominają zaufane domeny
- Ochronę przed podszywaniem się pod pracowni tj. przed wiadomościami, których nadawca znajduje się w katalogu G Suite, ale jego adres e-mail nie jest uwierzytelniony w domenie (ani aliasie domeny) firmy użytkownika
- Ochronę przed -mailami przychodzącymi, których nadawca podszywa się pod konto w domenie użytkownika
- Ochronę przed wszystkimi nieuwierzytelnionymi e-mailami
- Ochronę grup dyskusyjnych przed e-mailami przychodzącymi, których nadawca podszywa się pod konto w domenie użytkownika

4.7.3. **Apple**

Lista zabezpieczeń. Apple w dokumentach bezpieczeństwa nie deklaruje funkcjonalności dedykowanych do zapewnienia bezpieczeństwa przed złośliwym oprogramowaniem w związku z korzystaniem z usługi iCloud Mail. Apple zarządzając zabezpieczeniami przed złośliwym oprogramowaniem kładzie nacisk na bezpieczeństwo aplikacji, które w obecnie stosowanej architekturze urządzeń Apple stanowią punkt krytyczny.

Zgodnie z oświadczeniem Apple zamieszczonym w dokumencie „Bezpieczeństwo Platform Apple” (https://manuals.info.apple.com/MANUALS/1000/MA1902/pl_PL/apple-platform-security-guide-pl.pdf - str. 70-71, Apple stosuje następujące zabezpieczenia dla urządzeń lub aplikacji w celu ochrony przed złośliwym oprogramowaniem.

Wskazówki – dobre praktyki. Apple na swojej stronie internetowej podaje wskazówki, co należy robić, jeżeli otrzymamy podejrzany mail (https://support.apple.com/pl-pl/HT204759) W przypadku otrzymania podejrzanej wiadomości należy „przesłać” taką informację na wskazany adres firmy Apple (reportphishing@apple.com) by uchronić innych użytkowników przez ewentualnymi nadużyciami.

Apple, w odróżnieniu od Microsoft czy Google, nie deklaruje dedykowanych narzędzi typu anti-malware zapewniających bezpieczeństwo w usłudze iCloud Mail. Trzeba jednak przy tym wziąć pod uwagę, że Apple tworzy tzw. środowisko zamknięte, przeznaczone dla urządzeń produkcji Apple, gdzie Apple kontroluje zarówno urządzenia jak i oprogramowanie, które można na nich umieszczać, projektując przy tym na wstępie narzędzia zapewniające bezpieczeństwo i prywatność korzystania z tego środowiska. Stąd, jak się powszechnie przyjmuje i jak się nam wydaje, środowisko iOS cechuje się znacznie mniejszym ryzykiem zainfekowania złośliwym oprogramowaniem niż środowisko Windows czy Android.

4.8. Uwierzytelnianie użytkowników

Korzystanie z usługi email w bezpieczny sposób wymaga, aby dostęp do poczty był chroniony poprzez proces uwierzytelniania użytkownika tzn. w taki sposób, aby nie miał do niej dostępu każdy.

Podstawowym narzędziem uwierzytelnienia są login oraz indywidualne hasło użytkownika. W ten sposób dostęp do danych przetwarzanych za pomocą usługi email ma tylko konkretny użytkownik, pod warunkiem, że dane do logowania znane są tylko temu użytkownikowi. Dobrym standardem jest uwierzytelnianie dwuskładnikowe (2FA = *two factor authentication*, MFA = *multi factor authentication*, SCA = *strong customer authentication*), które umożliwiają wszyscy omawiani dostawcy.

Weryfikacja dwuetapowa (nazywana też uwierzytelnianiem dwuskładnikowym) dodatkowo zabezpiecza konto np. na wypadek kradzieży hasła, ponieważ wymaga:

a) informacji (np. nazwa użytkownika i hasło);

b) czegoś co się ma (np. telefonu, na który przychodzi sms uwierzytelniający).

W W przypadku przetwarzania danych z wykorzystaniem urządzeń mobilnych, przy ryzyku zgubienia lub kradzieży tych urządzeń, oraz w szczególności, gdy na naszej poczcie znajdują się szczególnie chronione informacje, w tym informacje objęte tajemnicą zawodową weryfikacja dwuetapowa powinna być włączona dla celu autoryzacji nowych urządzeń jak i dla celu zmiany danych dostępowych (takich, które zapewniają kontrolę nad kontem), takich jak login, hasło, email uwierzytelniający, numer telefonu uwierzytelniający.

4.8.1. **Microsoft**

Microsoft zapewnia proces uwierzytelniania użytkowników usług poprzez sam login i hasło (*single factor authentication* - SFA) lub z użyciem dodatkowego składnika – np. jednorazowego kodu weryfikacyjnego, telefonu, aplikacji The Microsoft Authenticator (*multi factor authentication* - MFA[58]). Uwierzytelnienie chroni przed nieuprawnionym dostępem do konta zarejestrowanego użytkownika, np. w przypadku fizycznego przejęcia sprzętu. MFA jest oczywiście bezpieczniejszą metodą uwierzytelniania niż uwierzytelnienie jednoskładnikowe. Microsoft udostępnia obie opcje, a decyzja o uruchomieniu opcji MFA zależna jest od klienta usługi. Microsoft oferuje także uwierzytelnienie użytkowników w modelu *single sign-on*, czyli z wykorzystaniem osobnej usługi dostawy tożsamości.

Proces uwierzytelnienia następuje poprzez usługę Microsoft – *Azure Active Directory*[59], niezależnie od tego, kto jest dostawcą tożsamości.

Wniosek: Poczta Microsoft zapewnia bezpieczne logowanie.

4.8.2. **Google**

Podobnie jak Microsoft, Google chroni dane swoich użytkowników przed nieautoryzowanym dostępem poprzez stosowanie weryfikacji za pomocą loginu i hasła.

Włączenie weryfikacji dwuetapowej leży po stronie administratora i może zostać włączone za pomocą konsoli administracyjnej.

Metody weryfikacji dwuetapowej, które oferuje Google są następujące[60]:

a) klucze bezpieczeństwa

b) potwierdzenie od Google

c) Google Authenticator

d) Kody zapasowe

e) SMS lub połączenie głosowe

Wniosek: Poczta Google zapewnia bezpieczne logowanie.

[58] https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/multi-factor-authentication-microsoft-365?view=o365-worldwide
[59] https://docs.microsoft.com/en-us/office365/enterprise/about-office-365-identity
[60] https://support.google.com/a/answer//175197#bestpractices

4.8.3. **Apple**

Apple umożliwia uwierzytelnianie dwuskładnikowe (dwupoziomowe) dla aplikacji zarejestrowanych na komputerze lub przy logowaniu się do swojego konta mail z wykorzystaniem strony www. Uwierzytelnianie dwupoziomowe obejmuje logowanie się za pomocą Apple ID oraz hasła, wraz z potwierdzeniem logowania przez otrzymany zaufany kod. Zaufany kod możne być wyświetlany automatycznie na zaufanych urządzeniach (np. na iPhone radcy) lub kod może być przesłany w formie SMS na zaufany numer telefonu lub podany za pomocą automatycznego połączenia[61].

Uwierzytelnianie dwupoziomowe konta ID można włączyć z poziomu urządzeń firmy Apple lub przez przeglądarkę internetową[62]. Niektóre konta Apple ID utworzone w systemie iOS 10.3 lub macOS 10.12.4 albo nowszym domyślnie są zabezpieczone przy użyciu uwierzytelniania dwupoziomowego. W takim przypadku uwierzytelnianie dwupoziomowe jest już włączone. W przypadku tworzenia konta Apple ID przy wykorzystywaniu z innego systemu lub korzystania z usługi za pomocą strony internetowej, należy dodatkowo włączyć uwierzytelnianie dwupoziomowego[63]. Domyślnie dostęp bez uwierzytelniania dwuskładnikowego do konta jest możliwy na zaufanych urządzeniach, gdzie został już utworzony lub zaufany adres poczty mail.

Wniosek: Poczta Apple zapewnia bezpieczne logowanie.

4.9. Zarządzanie dostępami i uprawnieniami użytkowników oraz administratorów

Klient usługi email powinien mieć możliwość samodzielnego zarządzania dostępami użytkowników oraz zakresem ich uprawnień, w celu wdrożenia wewnętrznego systemu zarządzania bezpieczeństwem informacji w odniesieniu do tych usług.

4.9.1. **Microsoft**

Microsoft pozwala w pełni zarządzać użytkownikami usługi, w tym tworzyć i usuwać użytkowników oraz nadawać im określone uprawnienia, w ramach usług, w tym administratorów lub zwykłych użytkowników. Pozwala to skutecznie zarządzać bezpieczeństwem informacji w organizacji.

4.9.2. **Google**

Podobnie jak Microsoft, Google pozwala dowolnie zarządzać dostępami i uprawnieniami użytkowników G-Suite. Google rozpoznaje role użytkowników, administratora, superadministratora, jak również pozwala na udzielanie niestandardowych ról administratora.

4.9.3. **Apple**

Zarządzanie urządzeniami. W ramach usługi Apple Business Manager radca prawny wykorzystujący urządzenia Apple w organizacji może automatycznie wdrażać i zarządzać urządzeniami mobilnymi swoich współpracowników. Zarządzanie dostępami i uprawnieniami w ramach usług oferowanych przez Apple, oparte jest na odpowiednim konfigurowaniu Apple ID.

Zarządzane Apple ID. W ramach usługi Apple Business Manager organizacja może utworzyć tzw. zarządzane Apple ID, które służą do logowania się do dedykowanych urządzeń użytkowników. Zarządzane Apple ID mogą być utworzone przez korzystanie z uwierzytelnionych nazw użytkowników i haseł usług Microsoft Azure Active Directory lub za pomocą ręcznie utworzonych kont. Każde konto w usłudze Apple Business Manager ma co najmniej jedną rolę określającą, co może zrobić użytkownik będący posiadaczem konta[64].

Role w organizacji. Apple w ramach usługi Apple Business Manager umożliwia dla każdego zarządzanego Apple ID przypisanie jednej z następujących ról: administrator, menedżer użytkowników, menedżer urządzeń, menedżer zawartości, personel[65].

4.10. Ciągłość i dostępność usług

Usługi poczty elektronicznej, w tym w ramach usług chmurowych, stanowią dzisiaj podstawowe narzędzia pracy także radców prawnych. Dlatego ich niedostępność, choćby czasowa może mieć istotny wpływ na wykonywanie tej pracy. W teorii, radcy mogą samodzielnie zapewnić ciągłość

[61] https://support.apple.com/pl-pl/HT204915
[62] https://support.apple.com/pl-pl/HT205075
[63] https://support.apple.com/pl-pl/HT204915
[64] https://support.apple.com/pl-pl/guide/apple-business-manager-m/tes78b477c81/1/web/1
[65] https://support.apple.com/pl-pl/guide/apple-business-manager/apd352f2e0ae/web

działania w zakresie tych usług poprzez zapewnienie sobie równoległego dostępu do rozwiązań alternatywnych – np. odrębnej, dostarczanej przez innego dostawcę skrzynki pocztowej. Najbezpieczniej, najwygodniej i najefektywniej jednak, gdy rozwiązania w zakresie ciągłości działania zapewni nam dostawca usługi, niezależnie od własnych planów i środków w tym zakresie posiadanych przez klienta-użytkownika.

Warto zauważyć, że ciągłość i dostępność usług chmurowych, leży przede wszystkim w interesie samych dostawców omawianych tutaj usług. Działają oni na bardzo konkurencyjnym rynku, na którym, jak udowadnia nawet ta opinia, łatwo dostępne są podobne usługi innych dostawców. Co więcej, usługi globalnych graczy poddane są zainteresowaniu publicznemu i krytycznemu zainteresowaniu konkurencji, specjalistów jak i tzw. „specjalistów na forach". Wiarygodność staje się w przypadku usług globalnych istotnym czynnikiem ich bezpieczeństwa.

4.10.1. **Microsoft**

Szczegółowe zobowiązania Microsoft dotyczące gwarantowanego poziomu dostępności usług zawiera dokument Service Level Agreement for Microsoft Online Services z 1 czerwca 2020 r.[66] Nie wchodząc w szczegóły dotyczące obliczania wskaźnika dostępności usługi, dla każdej z analizowanych w opinii usług, w przypadku spadku wskaźnika poniżej 99,9% w danym miesiącu, użytkownikowi przysługuje zniżka na opłatę subskrypcyjną.

Microsoft zapewnia ciągłość działania swoich usług Online[67]m.in. poprzez stały monitoring poziomu świadczenia usług oraz nadmiarowość zasobów wykorzystywanych do ich dostarczania. Według danych prezentowanych przez Microsoft, dostępność usług Office 365 od 2017 roku nie spadła poniżej poziomu 99,97%[68].

4.10.2. **Google**

Zgodnie z dokumentem Service Level Agreement – Gwarancja jakości usług G Suite, Google zobowiązuje się do tego, aby interfejs internetowy usługi G Suite był dostępny dla klienta przez co najmniej 99,9 % czasu w danym miesiącu kalendarzowym[69].

4.10.3. **Apple**

Brak gwarancji dostępności. Apple w umowie Apple Business Manager (pkt. 7 – zastrzeżenia dotyczące gwarancji) oraz w regulaminie ogólnym (EULA) nie gwarantuje dostępności usług na określonym poziomie oraz nie gwarantuje, że usługa lub jakakolwiek jej funkcja lub część będzie działała prawidłowo lub będzie dostępna w jakiejkolwiek konkretnej lokalizacji. Apple nie gwarantuje, że korzystanie z usług będzie wolne od zakłóceń bez wskazywania umownego czasu niedostępności usługi. Jednocześnie Apple zastrzega sobie prawo modyfikacji, zawieszenia lub zaprzestania świadczenia usługi w dowolnym czasie bez powiadomienia użytkownika[70].

Ryzyko użytkownika. Apple wskazuje, że używanie lub brak możliwości używania usługi, jakiegokolwiek narzędzia lub funkcji, funkcjonalności dostępnych przy użyciu usługi bądź za jej pośrednictwem odbywa się na wyłączne ryzyko użytkownika. Użytkownik bierze na siebie ryzyko związane z jakością, wydajnością i dokładnością. Jednocześnie Apple *odrzuca wszelkie gwarancje i warunki dotyczące usługi, zarówno wyrażone wprost domniemane lub ustawowe, w tym między innymi, domniemane gwarancje i/lub warunki handlowe, jakości, przydatności do określonego celu, dokładności, niezakłóconego używania*[71].

Podsumowanie

Formalnie żaden z omawianych dostawców nie oferuje odpowiedzialności odszkodowawczej za niedotrzymanie parametrów usługi, zaś Apple nie oferuje w ogóle poziomu dostępności. Mimo to, w przypadku podmiotów takich jak omawiani dostawcy (liderów w zakresie usług email), oferowane warunki bezpieczeństwa są w naszej ocenie wystarczające.

---

[66] https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37

[67] https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity

[68] Ibidem

[69] https://gsuite.google.com/terms/sla.html

[70] https://www.apple.com/legal/enterprise/apple-business-manager/abm-pl.pdf str. 9

[71] Ibidem str. 8

W przypadku Apple, Google oraz Microsoft działa efekt skali. Są to podmioty oferujące wysokowartościową usługę dla setek milionów podmiotów za darmo (dla konsumentów) lub za opłatą nieproporcjonalnie niską względem kosztu, jaki organizacja musiałaby ponieść, aby zapewnić sobie usługę porównywalną parametrami technicznymi i organizacyjnymi (model chmurowy „one to many" a wręcz „one to masses"). Wiarygodność tych podmiotów jest lepszym zakładnikiem niezawodności niż kary i odpowiedzialność finansowa.

Paradoksalnie ograniczenia finansowe działają w modelu chmury publicznej na korzyść ciągłości działania usługi. Ewentualne roszczenia jednego z podmiotów nie grożą finansowej stabilności całej usługi a zatem ograniczone jest ryzyko „zakażenia" usługi dla pozostałych jej klientów.

Z drugiej strony, gdyby problemy z usługą związane byłyby z naruszeniem europejskich przepisów o ochronie danych osobowych, ograniczenia odpowiedzialności nie znalazłyby zastosowania w odniesieniu do roszczeń osób fizycznych tym dotkniętych (art. 82 RODO).

Podsumowując, odpowiedzialność reputacyjna każdego z omawianych dostawców związana z powszechnością[72] świadczonej przez nich usługi email, zapewnia w naszej ocenie wystarczającą, wysoką gwarancję niezawodności tej usługi.

4.11. Kopie zapasowe

Tworzenie kopii zapasowych informacji pozwala mitygować ryzyko ich utraty. Podobnie, jak w przypadku ciągłości działania, użytkownik – radca może podejmować samodzielnie działania w celu realizacji tego środka bezpieczeństwa – np. ręcznie archiwizować skrzynkę pocztową, obok dysku wirtualnego lub wspólnego przechowywać dane także w innej lokalizacji. Na pewno pomocne i bardziej skuteczne będą jednak narzędzia zapewniane bezpośrednio przez usługę i dostawcę.

4.11.1. **Microsoft**

Usługa Exchange Online nie zapewnia klasycznych funkcji backupu. Użytkownik nie ma wpływu na to, jak dostawca zarządza tą funkcją w ramach centrów przetwarzania danych, za pomocą których świadczy usługę. Microsoft deklaruje bezpieczeństwo przechowywanych danych i ochronę przed utratą poprzez zapewnienie ciągłości i dostępności usługi. Tradycyjne funkcje back-upu nie są zapewniane[73]. Użytkownik może jedynie samodzielnie zadbać o okresowe kopiowanie zawartości swojej skrzynki. Pomocnym narzędziem może być tutaj udostępniany przez Microsoft Exchange Online Archiving[74].

Dodatkowym narzędziem ochrony przed utratą danych są mechanizmy *soft* i *hard deletion*[75]. Istnieje możliwość odzyskania poszczególnych wiadomości lub całej skrzynki mailowej. Po usunięciu wiadomości lub skrzynki użytkownika, np. po usunięciu użytkownika, wiadomości lub skrzynka przechowywane są dalej do 30 dni w zależności od konfiguracji – tzw. *soft delete*. W tym okresie administrator ma możliwość ich przywrócenia za pomocą funkcjonalności oferowanych w usłudze. Dotyczy to sytuacji zwykłego usunięcia. Jeżeli Administrator usunie dane z wybraniem opcji permanentnego usunięcia, dane nie są dalej przechowywane. Możliwość przywracania pojedynczych wiadomości wymaga, aby taka opcja uruchomiona była w Exchange Online. Domyślnie jest ona włączona, z 14-dniowym okresem przechowywania, który można wydłużyć do 30 dni.

Po upływie okresu przechowania danych przez Microsoft po ich usunięciu, wiadomości lub skrzynka są całkowicie usuwane – tzw. *hard deletion*.

4.11.2. **Google**

G Suite podobnie jak Microsoft nie posiada wbudowanej funkcji back-up-u danych serwera email. Google również deklaruje bezpieczeństwo przechowywania danych w centrach w różnych lokalizacjach, ochronę przed utratą ciągłości działania i dostępności usługi. W zakresie tworzenia kopii zapasowych, Google oferuje użytkownikom G Suite możliwość samodzielnego ustawienia

[72] nie chodzi nam o „usługę powszechną" w rozumieniu prawnym
[73] https://docs.microsoft.com/en-us/exchange/back-up-email
[74] https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-archiving-service-description/archive-features
[75] https://docs.microsoft.com/en-us/exchange/recipients-in-exchange-online/delete-or-restore-mailboxes https://docs.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-user-mailboxes/recover-deleted-messages

tworzenia kopii zapasowych plików i synchronizowania ich z komputerem z systemem operacyjnym Mac OS lub Windows[76].

4.11.3. **Apple**

Apple podobnie jak Google oraz Microsoft nie oferuje funkcji dodatkowego back-up-u danych przetwarzanych w serwerze iCloud Mail.

Apple umożliwia tworzenie kopii zapasowej treści przetwarzanych w poczcie e-mail bezpośrednio na komputer. W przypadku korzystania z aplikacji Mail w systemie OS X 10.7.5 lub nowszym aplikacja ta umożliwia przenoszenie i kopiowanie wiadomości e-mail z usługi iCloud na komputer[77].

4.11.4. **Podsumowanie ogólne dla kopii zapasowych**

W naszej ocenie, brak wbudowanych funkcji backupu serwera email w omawiane usługi email nie stanowi problemu w działalności nawet większych kancelarii radcowskich. Niezawodność tych usług jest mimo to wystarczająca.

Omawiane usługi email mają wysoki poziom niezawodności związany z ich infrastrukturą, dostarczają wysoki poziom ochrony przed złośliwym oprogramowaniem oraz reagowanie na malware może być oparte także o odzyskiwanie danych z poszczególnych urządzeń użytkowników w kancelarii. Obecnie malware koncentruje się raczej na atakowaniu serwerów plików. W tradycyjnym modelu architektury informacji kancelaria powinna dysponować serwerem plików lub jego odpowiednikiem (np. Sharepoint), który to powinien podlegać backupowaniu. Email i serwer plików/jego odpowiednik stanowią wzajemnie swoje backupy w pewnym zakresie. Duże organizacje natomiast mogą stosować rozwiązania komplementarne, zapewniające pełne przechowywanie korespondencji wpływającej i wypływającej do organizacji, klasy „enterprise". Małe organizacje mogą polegać na kopiach danych (emaili) znajdujących się na urządzeniach lokalnych (laptopach, telefonach) jako formie backupu.

5. WIARYGODNOŚĆ DOSTAWCY – PODSUMOWANIE, INFORMACJE O PODATNOŚCIACH, CERTYFIKATY

Zgodnie z 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.*

Z powyższego wynika, że ważne jest, aby radca prawny decydując się na usługę email ocenił wiarygodność dostawcy tej usługi w zakresie bezpieczeństwa. Warunki bezpieczeństwa opisane powyżej w pkt 3) wskazują, że Dostawcy oferują wysoki i zaawansowany poziom technologii, która odpowiada za bezpieczeństwo usługi email. W celu potwierdzenia swojej wiarygodności jako podmiotu przetwarzającego, Microsoft, Google oraz Apple deklarują formalną zgodność z wymogami RODO oraz mających zastosowanie przepisów krajowych. Szereg zapewnień, oświadczeń i deklaracji Dostawców został wskazany w pkt X opinii – ŹRÓDŁA. Wiarygodność Dostawców należy również oceniać przez pryzmat medialnych doniesień o podatnościach jak i posiadanych przez nich certyfikatów bezpieczeństwa.

5.1. Medialne informacje o podatnościach

5.1.1. **Microsoft**

Usługi i oprogramowanie firmy Microsoft należą do tych najpopularniejszych i najpowszechniej wykorzystywanych na całym świecie. Tym samym należą one też do tych najczęściej testowanych i atakowanych. Naturalny jest tutaj proces ciągłego wykrywania podatności i ich łatania. Dopóki więc nie dochodzi do istotnych incydentów bezpieczeństwa, informacje o identyfikowanych i naprawianych lukach nie powinny powodować automatycznej rezygnacji z usługi. W ostatnim czasie nie pojawiły się informacje o istotnych problemach z bezpieczeństwem usług Microsoft 365.

5.1.2. **Google**

[76] https://support.google.com/drive/answer/2374987; https://support.google.com/a/answer/2490101?hl=pl
[77] https://support.apple.com/pl-pl/HT202736

Google to gigant technologiczny, który może pochwalić się stosunkowo dobrą opinią. Oczywiście zdarzają się doniesienia, z których wynika, że nie zawsze procedury bezpieczeństwa są na wymaganym poziomie, chociażby takie jak informacja o tym, że Google przechowywał hasła użytkowników jako zwykły tekst[78], jednak generalnie Gmail uważany jest za bezpieczny[79]. Potwierdza to także raport The Forrester dotyczący bezpieczeństwa zapewnianego przez dostawców usług aktualny na 2 kwartał 2019 r., który uznaje Google za światowego lidera w obszarze bezpieczeństwa danych.

5.1.3. **Apple**

Apple w swoich oświadczeniach wskazuje, że ochrona prywatności użytkowników ma nadrzędne znaczenie. Apple jest również tak postrzegany na rynku dostawców rozwiązań chmurowych jako wiarygodna firma, które nie dzieli się danymi zebranymi od użytkowników z reklamodawcami czy innymi podmiotami bez wiedzy i zgody użytkowników. Obecnie nie zostały udowodnione Apple celowe działania zmierzające do sprzedaży czy ograniczenia prywatności użytkowników.

Apple jest jednak firmą zorientowaną pierwotnie na rynek konsumencki. Z tego powodu nie zapewnia pełnego ekosystemu dla przedsiębiorstw ani nie dysponuje takimi narzędziami klasy korporacyjnej jak Microsoft czy nawet Google. W małych kancelariach zagadnienie to ma mniejsze znaczenie, jednak niepomijalne.

Błąd w aplikacji Mail dla iOS. Ostatnim doniesieniem medialnym w zakresie podatności aplikacji mail była sprawa nagłośniona przez ZecOps. Firma z Kalifornii zajmująca się cyberbezpieczeństwem i kryminalistyką wykryła, że opracowano złośliwy program, który wykorzystywał lukę w oprogramowaniu Apple dla poczty elektronicznej na iPhone'ach i iPad'ach. Obecnie sprawa jest rozwiązywana, a rzecznik prasowy Apple przyznał, że w najbliższej aktualizacji systemu zostanie wprowadzona poprawka do błędu[80].

5.1.4. **Rating UpGuard**

Według firmy UpGuard, do którego odwołuje się także firma konsultingowa Gartner, ogólna ocena cyberbezpieczeństwa rozwiązań dostawców przedstawia się następująco: Microsoft 827/950[81], Google 865/950[82], Apple 751/950[83].

5.2. Certyfikacje bezpieczeństwa

Miarodajne dla oceny bezpieczeństwa i wiarygodności dostawcy oraz usługi mogą być także posiadane przez te podmioty uznane i rozpoznawalne certyfikaty. Zewnętrzne audyty i certyfikacje podnoszą wiarygodność dostawcy i jego usługi.

5.2.1. **Microsoft**

Microsoft deklaruje, że jego usługi chmurowe posiadają m.in. certyfikaty zgodności z[84]:

- ISO 22301
- ISO 27001 - bezpieczeństwo informacji
- ISO 27017- bezpieczeństwo chmury
- ISO 27018 - prywatność chmury

---

[78] https://xopero.com/blog/pl/2019/05/29/windows-z-nowa-podatnoscia-hasla-z-g-suite-w-dokumencie-tekstowym-deszyfratory-jsworm-2-0-i-getcrypt/

[79] https://niebezpiecznik.pl/post/gmail-najbezpieczniejszy/

[80] https://mojmac.pl/2020/04/23/powazny-blad-w-mail-dla-ios-niebawem-bedzie-naprawiony/

[81] https://www.upguard.com/security-report/microsoft

[82] https://www.upguard.com/security-report/abc

[83] https://www.upguard.com/security-report/apple

[84] https://opdhsblobprod04.blob.core.windows.net/contents/5c7b3adccc6146cab42d4d0f775bec31/d5529b7c32036fc64b988e6f0eafe478?sv=2018-03-28&sr=b&si=ReadPolicy&sig=0QRwtOd7Uu9tjAogsy6WJUlvDi%2F%2Btu3ardABOhSzgEk%3D&st=2020-06-24T22%3A39%3A45Z&se=2020-06-25T22%3A49%3A45Z

5.2.2. **Google**

Google deklaruje, że posiada następujące certyfikaty, które potwierdzają zgodność przetwarzania danych w Google Cloud (w tym dla G Suite) z wymogami RODO i standardami branżowymi[85]:

- ISO 27001
- ISO 27017
- ISO 27018
- SOC 2, SOC 3 - Service and Organization Controls 2 (SOC 2) to ocena procedur kontrolnych w organizacji IT, która świadczy usługi; Service and Organization Controls 3.

5.2.3. **Apple**

Apple deklaruje, że w ramach usługi Apple Business Manager zapewnia odpowiedni stopień bezpieczeństwa co mają potwierdzać certyfikaty niezależnych audytorów zgodności z normami ISO 27001, ISO 27018.

VI. PODSUMOWANIE

Przeprowadzona analiza wskazuje, że radcowie prawni mogą wykorzystywać dla celów wykonywania zawodu usługę Exchange Online w ramach pakietu Microsoft 365 a także Gmail w ramach pakietu G-Suite, natomiast wątpliwe byłoby wykorzystywanie usługi iCloud Mail.

Wszystkie usługi email zapewniają wysoki poziom bezpieczeństwa (poufności i ciągłości), niemożliwy do osiągnięcia przez radcę w wersji „on premise", tym bardziej przy porównywalnych kosztach dla mikro lub małej firmy.

Warunki prawne Microsoft 365 i G-Suite są zgodne z wymaganiami RODO (przy tym potwierdzenie zgodności G-Suite wymaga nieco interpretacji) natomiast warunki prawne usługi Apple Business Manager trudno jednoznacznie uznać za zgodne z RODO.

W Microsoft 365 dane (korespondencja) są przechowywane w EOG, w G-Suite można i należy ustawić przechowywanie danych w EOG, natomiast w iCloud przechowywanie danych nie może zostać ograniczone do EOG. Ograniczenie przechowywania emalii do terenu EOG w usługach Microsoft 365 (Exchange Online) i G-Suite (Gmail) w naszej ocenie pozwala uznać, że dane osobowe w tych usługach są chronione odpowiednio. Natomiast na tle treści wyroku Schrems II ocena ryzyka naruszenia praw i wolności osób, których dotyczyłaby korespondencja email radcy, może doprowadzić do uznania, że dane te nie będą w usłudze iCloud podlegały ochronie odpowiedniej do ochrony wynikającej z prawa UE (RODO).

Należy pamiętać, że warunkiem legalności korzystania z którejkolwiek z usług dla celów wykonywania zawodu jest wykupienie usługi biznesowej przez radcę.

Rozszerzone wnioski wraz z informacją praktyczną, jak skonfigurować G-Suite, znajdują się na początku opinii.

VII. ŹRÓDŁA

6. PRZEPISY PRAWA

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**);

[85] https://static.googleusercontent.com/media/gsuite.google.com/pl//files/google-apps-security-and-compliance-whitepaper.pdf, https://cloud.google.com/security/gdpr/resource-center/pdf/googlecloud_gdpr_whitepaper_618.pdf

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 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

5) Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 16 lipca 2020 r. w sprawie C-311/18[86], (dalej: **Schrems II**)

6) Kodeks Etyki Radcy Prawnego

7. DOKUMENTACJA

Opinia została przygotowana z uwzględnieniem następującej dokumentacji oraz oświadczeń:

1. Dla usługi oferowanej przez Microsoft

1.1. Oświadczenie o ochronie prywatności (https://privacy.microsoft.com/pl-pl/privacystatement)

1.2. Dodatek dotyczący ochrony danych w ramach usług online Microsoft, lipiec 2020 (https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=DPA)

1.3. Regulamin świadczenia usług online, sierpień 2020 (https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46)

1.4. Microsoft 365 Compliance Offerings (https://opdhsblobprod04.blob.core.windows.net/contents/5c7b3adccc6146cab42d4d0f775bec31/d5529b7c32036fc64b988e6f0eafe478?sv=2018-03-28&sr=b&si=ReadPolicy&sig=dPVTMBsd3No2017NsaXpWNb%2BSP1LSAJs2mK3mkVHqL0%3D&st=2020-06-25T08%3A51%3A13Z&se=2020-06-26T09%3A01%3A13Z)

1.5. Umowa dotycząca Poziomu Usług Online Microsoft 1 sierpnia 2020 r. (https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37)

1.6. 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)

1.7. 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)

1.8. Deklaracja gdzie przechowywane są dane użytkowników (https://docs.microsoft.com/pl-pl/office365/enterprise/o365-data-locations?ms.officeurl=datamaps)

1.9. Deklaracja dotycząca stosowania SCC (https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-eu-model-clauses?view=o365-worldwide)

2. Dla usługi oferowanej przez Apple

2.1. Zasady Ochrony Prywatności (https://www.apple.com/legal/privacy/pl/)

[86] Treść wyroku: http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=10402470

2.2. Bezpieczeństwo platform Apple, Wiosna 2020 (https://manuals.info.apple.com/MANUALS/1000/MA1902/pl_PL/apple-platform-security-guide-pl.pdf)

2.3. Bezpieczeństwo aplikacji — omówienie (https://support.apple.com/pl-pl/guide/security/sec35dd877d0/1/web/1)

2.4. Umowa dotycząca usługi Apple Business Manager (https://www.apple.com/legal/enterprise/apple-business-manager/abm-pl.pdf)

2.5. Regulamin korzystania z usług Apple (https://www.apple.com/pl/legal/internet-services/icloud/pl/terms.html)

2.6. Podręcznik użytkownika aplikacji Mail (https://support.apple.com/pl-pl/guide/mail/welcome/mac)

2.7. Podręcznik użytkowania iCloud (https://support.apple.com/pl-pl/guide/icloud/mm74e822f6de/icloud)

2.8. Omówienie kwestii bezpieczeństwa w usłudze iCloud (https://support.apple.com/pl-pl/HT202303)

2.9. Standardowe Klauzule Umowne (https://www.apple.com/legal/enterprise/data-transfer-agreements/datatransfer-pl.pdf)

3. Dla usługi oferowanej przez Google

3.1. Podsumowanie dotyczące usług G Suite (opis usług G Suite): https://gsuite.google.com/terms/user_features.html

3.2. Regulamin usługi bezpłatnej: https://gsuite.google.com/terms/standard_terms_checkout.html

3.3. Regulamin usług dla firm: https://gsuite.google.com/terms/2013/1/premier_terms.html

3.4. Szczegółowe warunki korzystania z usługi G Suite: https://gsuite.google.com/terms/service-terms/

3.5. Umowa G Suite (online): https://gsuite.google.pl/intl/pl/terms/2013/1/premier_terms.html

3.6. Umowa G Suite (online) dla użytkowników z EEA: https://admin.google.com/terms/apps/1/11/en/premier_terms_eea.html

3.7. Umowa Cloud Identity Agreement: https://cloud.google.com/terms/identity/na_terms

3.8. Umowa powierzenia przetwarzania danych: Aneksy do umów G Suite i Cloud Identity dotyczące spełniania wymogów jako metody spełnienia wymagań zgodności i bezpieczeństwa RODO: https://gsuite.google.com/terms/dpa_terms.html

3.9. Standardowe klauzule umowne: https://gsuite.google.com/terms/mcc_terms.html

3.10. Jak Google dba o bezpieczeństwo i prywatność Twojej organizacji?: https://support.google.com/a/answer/60762?hl=pl&ref_topic=7558840

3.11. Informacja dotycząca zgodności Google Cloud z RODO: https://cloud.google.com/security/gdpr/

3.12. General Data Protection Regelation - Google Cloud Whitepaper: https://cloud.google.com/security/gdpr/resource-center/pdf/googlecloud_gdpr_whitepaper_618.pdf

3.13. Google Cloud GDPR Quick Reference Guide: https://services.google.com/fh/files/misc/googlecloud_gdpr_quickreferenceguide_oct2018.pdf

3.14. G Suite Data Implementation Guide: https://cloud.google.com/files/gsuitedataprotectionimplementationguide_012019.pdf

3.15. Deklaracja środków bezpieczeństwa infrastruktury Google:

https://cloud.google.com/security/infrastructure/design/resources/google_infrastructure_whitepaper_fa.pdf

https://services.google.com/fh/files/misc/security_whitepapers_march2018.pdf

3.16. Deklaracja szyfrowania danych w spoczynku: https://cloud.google.com/security/encryption-at-rest/default-encryption/resources/encryption-whitepaper.pdf

3.17. Deklaracja szyfrowania danych w transmisji: https://cloud.google.com/security/encryption-in-transit/resources/encryption-in-transit-whitepaper.pdf

3.18. Deklaracja szyfrowania danych dla usługi G Suite – G Suite Encryption Whitepaper: https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf

3.19. Google Cloud Security and Compliance Whitepaper: https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-cloud-security-and-compliance-whitepaper.pdf

3.20. Google Cloud liderem w raporcie firmy Forrester Research za II kwartał 2019 r. dotyczącym dostawców rozwiązań z zakresu bezpieczeństwa danych: The Forrester Wave™: Data SecurityPortfolio Vendorors, Q2 2019: https://cloud.google.com/forrester-data-security-portfolio-security-wave/

Pod uwagę wzięto również szereg doniesień medialnych dotyczących omawianych usług. Opinia uwzględnia treść ww. dokumentów i deklaracji na dzień jej sporządzenia.

* * *

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	Michał Ćwiakowski	Katarzyna Kloc	Patrycja Szurmak
radca prawny CIPP/E	*adwokat certyfikowany auditor wiodący ISO 27001*	radca prawny *certyfikowany auditor wiodący ISO 27001*	*aplikantka radcowska*

O Autorach

MACIEJ GAWROŃSKI

Radca prawny, Certified International Privacy Professional Europe of International Association of Privacy Professionals (CIPP/E IAPP), partner Gawroński & Partners. 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. Skutecznie reprezentował klientów w setkach spraw, w tym o wartości przekraczającej 10 miliardów złotych.

MICHAŁ ĆWIAKOWSKI

Adwokat, Szef Praktyki Regulacji Bankowych i Finansowych Gawroński & Partners. Pracował w największych bankach w Polsce, w obszarze prawnym i ryzyka, oraz w 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. Prowadził kompleksowe projekty wdrożenia regulacji oraz audytów powdrożeniowych. 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. Wykładowca podyplomowych studiów compliance Szkoły Głównej Handlowej. Certyfikowany audytor wiodący systemów zarządzania bezpieczeństwem informacji zgodnie z PN-EN ISO/IEC 27001:2017.

KATARZYNA KLOC

Radca prawny, partner, certyfikowany auditor wiodący ISO 27001

Specjalistka zagadnień z zakresu ochrony danych osobowych oraz prawa nowych technologii.

Posiada wieloletnie, bogate doświadczenie w doradztwie prawnym z zakresu ochrony prywatności i danych osobowych w rankingowych międzynarodowych kancelariach prawnych w tej dziedzinie. Katarzyna doradza klientom z wielu sektorów gospodarki, takich jak sektor bankowy, technologiczny, finansowy czy e-commerce. Posiada doświadczenie w doradztwie w zakresie ochrony własności intelektualnej, prawa ochrony konsumentów, e-commerce oraz zagadnień prawnych związanych z IT. Absolwentka Wydziału Prawa i Administracji Uniwersytetu im. Marii Curie-Skłodowskiej w Lublinie. Ukończyła również podyplomowe studia z zakresu prawa gospodarczego i handlowego. Wykładowca na studiach podyplomowych w Szkole Głównej Handlowej i na Uczelni Łazarskiego.

PATRYCJA SZURMAK

Associate Gawroński & Partners. Patrycja specjalizuje się w obszarze ochrony danych osobowych, nowych technologii, własności intelektualnej, eCommerce oraz telemedycyny. Zdobywała doświadczenie w międzynarodowych korporacjach oraz w butikowych polskich kancelariach. W Gawroński & Partners 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 systemów IT, w tym z wykorzystaniem cloud computingu. 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. Współautorka książek i artykułów z dziedziny ochrony danych osobowych, wykłada analizę ryzyka na Uczelni Łazarskiego.

BEZPIECZEŃSTWO DANYCH PRZECHOWYWANYCH PRZEZ RADCÓW PRAWNYCH W WYBRANYCH CHMURACH

Kielce

8 lipca 2020 r. (zaktualizowano na dzień 25 lipca 2020 r.)

Spis treści

I. 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 – liderzy jutra 2019.

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.

II. PRZEDMIOT INFORMACJI

1. W niniejszym opracowaniu omawiamy warunki przechowywania plików w chmurach wybranych dostawców (ze szczególnym uwzględnieniem kwestii szyfrowania danych) oraz przedstawiamy opinię dotyczącą tego, czy radcowie prawni, wykonując swój zawód, mogą korzystać z tego rodzaju usług.

2. Przede wszystkim przeanalizowaliśmy deklaracje dostawców dotyczące szyfrowania danych przechowywanych w chmurze w celu ustalenia, czy poziom bezpieczeństwa gwarantuje zachowanie odpowiedniej poufności, a także zweryfikowaliśmy kwestie zgodności działania wybranych dostawców z przepisami o ochronie danych osobowych (w szczególności RODO).

3. W naszym opracowaniu omówione zostały usługi świadczone przez:

   1) Google – w ramach usługi Google Drive (Dysk Google), która jest częścią pakietu G Suite;

   2) Microsoft – w ramach usługi OneDrive, która jest samodzielną usługą, ale może być również częścią pakietu Microsoft 365[87];

   3) Apple – w ramach usługi iCloud Drive, która jest częścią pakietu iCloud.

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

5. Część informacji znajduje się w tekstach zamieszczonych na stronach internetowych i nie jest bezpośrednio dostępna w plikach, które można pobrać na dysk. W takim przypadku zamieszczaliśmy w przypisach bezpośrednie linki odsyłające do stron internetowych, na których odszukaliśmy

[87] Obecnie pakiet ten nazywa się Microsoft 365, dawniej nazywał się Office 365.

powoływane informacje. Informacje podawane przez dostawców są co pewien czas aktualizowane, dlatego zachęcamy do ich samodzielnej lektury i weryfikacji, czy nie zmieniły się one w porównaniu do tych wersji, które były opublikowane w momencie sporządzania przez nas opracowania.

6. W przypadku gdy powoływane przez nas informacje były ujęte w dokumentach lub materiałach, które można pobrać na dysk, podawaliśmy datę opracowania takiego dokumentu (o ile była dostępna), a także zamieszczaliśmy bezpośredni link do tego dokumentu lub materiału, ewentualnie link do strony, z której można go pobrać.

7. Opracowanie, którego pierwotna wersja została sporządzona w oparciu o stan prawny obowiązujący na dzień 8 lipca 2020 r., zaktualizowaliśmy tak by uwzględniało stan prawny na dzień 25 lipca 2020 r. Potrzeba aktualizacji opracowania była wynikiem wydania przez Trybunał Sprawiedliwości Unii Europejskiej wyroku z dnia 16 lipca 2020 r. w sprawie C-311/18 (tzw. sprawa Schrems II).

8. Wyrok ten ma kluczowe znaczenie dla podmiotów, które przekazują dane osobowe do USA, w tym dla podmiotów, które korzystają z usług przedsiębiorców przetwarzających dane właśnie w Stanach Zjednoczonych.

9. Wyjaśnienia będzie więc wymagało, jaki wpływ ma orzeczenie TSUE na radców prawnych korzystających z usług podmiotów przekazujących dane do USA (w tym dostawców usług chmurowych).

III. CHMURA W DZIAŁALNOŚCI RADCÓW PRAWNYCH

8. [informacje wstępne]

10. Ostatnie miesiące, w czasie których wiele kancelarii zdecydowało się na przejście w tryb częściowo zdalnej pracy, dobitnie pokazały, że branża prawnicza nie jest wyjątkiem, który obroni się przed rewolucją związaną z koniecznością coraz szerszego stosowania nowych technologii w biznesie. Oczywiście wielu radców prawnych od lat korzysta z narzędzi i aplikacji ułatwiających pracę przez internet, jednak z różnych względów nie był to standard we wszystkich kancelariach.

11. Okazało się, że może jednak zdarzyć się sytuacja, w której takie narzędzia okażą się potrzebne nie tyle, po to aby efektywniej pracować, ale aby pracować w ogóle. Przykładem niech będą chociażby narzędzia do prowadzenia wideokonferencji, które szybko stały się substytutem spotkań osobistych czy rozwiązania umożliwiające dostęp do akt sprawy bez konieczności wizyty w biurze kancelarii.

12. Zakładamy, że ten przyspieszony kurs nowych technologii będzie miał swoje trwałe konsekwencje, to znaczy że sporo z tych rozwiązań - zastosowanych w czasie pandemii „z przymusu" - będzie stosowanych nawet po całkowitym zniesieniu obostrzeń. Wielu radców prawnych miało okazję przekonać się, że są one bardzo wygodne i znacząco usprawniają pracę.

13. Jednym z narzędzi, których stosowanie okazało się ostatnio bardzo przydatne jest tzw. chmura obliczeniowa (cloud computing) umożliwiająca m.in. przechowywanie plików na zewnętrznych serwerach i uzyskiwanie dostępu do tych plików za pośrednictwem internetu, bez względu na miejsce, w którym użytkownik się znajduje.[88]

14. W praktyce można spotkać się m.in. z określeniami chmury publicznej, prywatnej i hybrydowej.[89]

15. Chmura publiczna to usługa ogólnodostępna, z której mogą korzystać wszystkie zainteresowane podmioty. Taki rodzaj chmury zapewniają omawiani w tym opracowaniu dostawcy, a także inne podmioty takie jak np. Dropbox, Amazon, ale również krajowi usługodawcy (zachęcamy również do zapoznania się z oferowanymi przez nich warunkami świadczenia usługi). Przewagą tej chmury jest to, że jest ona łatwo dostępna, można relatywnie szybko wdrożyć jej stosowanie w organizacji, a jej koszty nie są zazwyczaj wysokie. Zwykle dostawcy chmur publicznych oferują jednak standardowe rozwiązania dla wszystkich użytkowników. Trzeba się więc do nich dostosować i nie ma możliwości indywidualizowania usługi. Tym rodzajem chmury zajmiemy się w niniejszym opracowaniu.

16. Chmura prywatna to z kolei chmura konkretnego przedsiębiorstwa lub instytucji. Z jej posiadaniem wiąże się konieczność utrzymania własnych serwerów, co oczywiście zwiększa potencjalne koszty i wymaga nadzorowania poprawności jej działania. Daje jednak możliwość dostosowania usługi do indywidualnych potrzeb przedsiębiorstwa.

17. Chmura hybrydowa łączy chmurę publiczną i prywatną. Dane użytkownika są przenoszone wtedy między częścią publiczną a prywatną. Takie rozwiązanie pozwala na przykład przechowywać poufne dokumenty w prywatnej części chmury, a pozostałe materiały w chmurze publicznej.

18. Chmura jest modelem przetwarzania danych, z którego można korzystać przy użyciu internetu, w szczególności przez przesyłanie i przechowywanie danych. Model ten opiera się na współdzieleniu zasobów informatycznych (np. serwerów) zapewnianych przez dostawcę usługi. W dużym uproszczeniu można powiedzieć, że chmura umożliwia m.in. przesyłanie („upload") plików na serwer dostawcy i uzyskanie do nich dostępu z różnych urządzeń. Mogą to być urządzenia tej samej osoby, ale równie dobrze mogą to być urządzenia innych osób (np. pracowników).

19. Po pierwsze, radca prawny może więc mieć ze swoich urządzeń dostęp do wszystkich plików przesłanych do chmury. Dzięki temu nie musi pamiętać o zapisywaniu plików na zewnętrznych nośnikach, jeśli chce na przykład kontynuować pracę nad pismem procesowym na innym komputerze lub chce otworzyć dokument na telefonie lub tablecie.

---

[88] Na temat prawnych kwestii stosowania chmury zob. A. Krasuski, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Wolters Kluwer Polska 2018.

[89] Więcej na temat chmury publicznej, prywatnej i hybrydowej zob. np. https://azure.microsoft.com/pl-pl/overview/what-are-private-public-hybrid-clouds/, dostęp na dzień 8 lipca 2020 r.

20. Po drugie, można udostępnić pliki (w tym na przykład skany akt lub projekty pism procesowych) wszystkim (lub wybranym) prawnikom w kancelarii. Znacznie ułatwia to pracę, szczególnie w większych zespołach i kancelariach, które mają biura w różnych miastach. Jeśli nad daną sprawą pracuje kilka osób, to mogą mieć one równoczesny dostęp do zdigitalizowanych akt sprawy. Niektóre chmury umożliwiają również pracę wielu osób nad tym samym plikiem w tym samym czasie, dzięki udostępnianiu edytora tekstu działającego online (tak właśnie częściowo powstało to opracowanie). Równoległa praca całego zespołu nad pismem procesowym czy umową pozwala na optymalizację czasu pracy i przyspieszenie terminów realizacji projektów. Poszczególne pliki lub całe foldery z plikami można również udostępniać klientom, dzięki czemu mogą oni na bieżąco zapoznawać się z postępem prac, bez konieczności prowadzenia rozmów telefonicznych czy korespondencji mailowej.

21. Dostęp do chmury możliwy jest zwykle z poziomu przeglądarki internetowej. W przypadku niektórych usług (np. Google Drive i OneDrive) można zainstalować na komputerze aplikację, która tworzy foldery synchronizujące się automatycznie z chmurą. Zapisywanie plików w takich folderach nie różni się niczym od zapisu w jakimkolwiek innym miejscu na dysku komputera. Działająca w tle aplikacja automatycznie przesyła pliki na serwery dostawcy. Jest to więc bardzo wygodne rozwiązanie. Aplikację taką można zainstalować również na telefonie czy tablecie.[90] Będzie ona wtedy synchronizowała pliki także między urządzeniami.

22. Choć, przynajmniej na razie, chmura nie zastąpi prowadzenia papierowych akt sprawy, to nawet częściowa digitalizacja dokumentacji może przyczynić się do usprawnienia procesów przepływu informacji i obiegu dokumentów w kancelarii.[91]

9. [bezpieczeństwo chmury]

23. Kwestią, która od lat pojawia się jako przedmiot dyskusji wśród radców prawnych zainteresowanych tematem chmury jest sprawa bezpieczeństwa i poufności przechowywanych plików.

24. Ryzyko, że ktoś niepowołany uzyska dostęp do plików, które przechowujemy wyłącznie lokalnie – na własnym komputerze, nie jest wysokie i wynika w największej części z możliwości zgubienia lub kradzieży takiego komputera, ewentualnie z możliwości awarii.[92]

---

[90] Korzystanie z takich ułatwień wymaga jednak odpowiedniego zabezpieczenia tych urządzeń mobilnych (np. przynajmniej kodem służącym do odblokowywania), po to aby w sytuacji zgubienia lub kradzieży urządzenia, osoba nieupoważniona nie uzyskała dostępu do plików.

[91] W sprawie wykorzystania chmury w kancelariach radców prawnych zob. również: *Chmura w kancelarii prawnej czy kancelaria prawna w chmurze? Publikacja po konferencji Krajowej Izby Radców Prawnych*, 20 czerwca 2018 r., http://kirp.pl/wp-content/uploads/2018/10/01-publikacja-pokonferencyjna-dla-kirp-2018-pages.pdf, dostęp na dzień 8 lipca 2020 r.

[92] Trzeba jednak pamiętać, że takie podejście powoduje, że w przypadku utraty komputera (np. awarii dysku) wszystkie pliki mogą zostać utracone. Należałoby zatem zadbać o cykliczne wykonywanie kopii bezpieczeństwa, które powinny być przechowywane w innym miejscu niż ten komputer.

25. W przypadku chmury publicznej, pliki są przechowywane na serwerach zewnętrznych dostawców. Użytkownik nie ma kontroli nad środkami bezpieczeństwa, które taki dostawca stosuje. Dodatkowo pliki są przesyłane do chmury przez internet, co rodzi dodatkowe ryzyko związane z potencjalnym atakiem podczas ich transferu.

26. Są to ryzyka, które występują także w przypadku innych usług internetowych, takich jak chociażby poczta elektroniczna. Nikt nie kwestionuje jednak przy tym samej dopuszczalności korzystania z poczty elektronicznej. Dyskusyjne może być jedynie to, czy konkretna poczta elektroniczna spełnia odpowiednie warunki. W naszej ocenie podobna konkluzja powinna zostać wyrażona w stosunku do chmury. Oczywiście zdajemy sobie sprawę, że chmura jest bardziej kontrowersyjnym tematem z uwagi na to, że potencjalnie może być tam przechowywanych więcej informacji objętych tajemnicą zawodową niż w przypadku skrzynki pocztowej (przykładowo kancelarie korzystające z chmury mogą przechowywać w niej skany całych akt sprawy, a nie tylko projekty pism procesowych).

27. Kolejną wątpliwością, która wiąże się z chmurą jest możliwość uzyskania przez dostawcę dostępu do przechowywanych w niej danych. Jak wyjaśnimy w dalszej części opracowania, w standardowych przypadkach chmury publicznej dostawca ma potencjalną możliwość wglądu do plików, które przechowuje dla użytkowników. Oznacza to, że teoretycznie może zapoznać się z ich treścią. Skoro zaś sam może się z nimi zapoznać, to może również przekazać je podmiotom trzecim. Taka sytuacja powoduje oczywiście konieczność zadania pytania o zgodność korzystania z usług cloudowych z obowiązkiem zachowania tajemnicy zawodowej.

28. W tym opracowaniu chcieliśmy zwrócić uwagę właśnie m.in. na identyfikację ryzyk związanych z chmurą, po to żeby można było podjąć bardziej świadomą decyzję o korzystaniu z takiego narzędzia, rezygnacji z niego lub korzystaniu, ale przy dodatkowych środkach bezpieczeństwa.

10. [chmura a przetwarzanie danych osobowych]

29. Oprócz dokumentów czy materiałów objętych tajemnicą zawodową, w chmurze kancelarii będą przechowywane niemal zawsze dane osobowe – zarówno klientów radcy prawnego, jak i innych osób (np. uczestników postępowania, strony przeciwnej itp.), co oznacza oczywiście, że dochodzi do przetwarzania danych osobowych. Nie sposób wyliczyć wszystkich kategorii danych, które mogą być przetwarzane przez kancelarie w ten sposób. Będzie to oczywiście zależało od konkretnych plików, które zostaną przesłane na wirtualny dysk.

30. Dostawca będzie co do zasady podmiotem przetwarzającym dane osobowe w imieniu administratora, który korzysta z chmury (np. radcy prawnego). W relacji radca prawny – dostawca dojdzie więc do powierzenia przetwarzania danych osobowych w rozumieniu art. 28 RODO.

31. Przesądzenie, że w ramach chmury dochodzi do przetwarzania danych osobowych i, że odbywa się to w modelu powierzenia przetwarzania danych osobowych ma swoje daleko idące konsekwencje. W tym opracowaniu poruszymy, więc również kwestię oceny zgodności poszczególnych usług z RODO.

IV. OTOCZENIE PRAWNE

11. [informacje wstępne]

32. Oczywistym jest, że radcowie prawni powinni z dużą uwagą podchodzić do wyboru chmury, w której zamierzają przechowywać pliki, skoro mają się tam znaleźć informacje objęte tajemnicą zawodową oraz dane osobowe.

33. Radcowie prawni muszą w tym zakresie zwrócić uwagę na obowiązki wynikające z przepisów ustawy o radcach prawnych, Kodeksu Etyki Radcy Prawnego oraz RODO.

34. Odpowiedni wybór dostawcy chmury wiąże się z obowiązkiem przestrzegania tajemnicy zawodowej (art. 23 KERP, § 6 ust. 1 Regulaminu) oraz zapewnienia bezpieczeństwa danych osobowych (art. 5 ust. 1 lit. f RODO).

12. [zasady etyki]

35. Przywołując regulacje dotyczące etyki, które radca prawny powinien uwzględnić, należy w pierwszej kolejności wskazać na art. 3 ust. 3 ustawy o radcach prawych. Zgodnie z tą regulacją radca prawny jest obowiązany zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzieleniem pomocy prawnej.

36. Dodatkowo przepisy związane z tajemnicą zawodową zawiera również Kodeks Etyki Radcy Prawnego. Zgodnie z 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).

37. Tajemnica zawodowa obejmuje również wszelkie tworzone przez radcę prawnego dokumenty (art. 15 ust. 2 KERP). Dochowanie tajemnicy zawodowej jest prawem i obowiązkiem radcy prawnego (art. 9 KERP). 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 KERP).

38. Warto również przywołać art. 35 pkt 6 KERP zgodnie, z którym m.in. radca prawny może wykonywać czynności zawodowe drogą elektroniczną, jeśli poprzez okresową archiwizację zabezpiecza i dba o dostępność danych przetwarzanych drogą elektroniczną.

39. Przepisem, którego nie można pominąć z uwagi na to, że zawiera on najbardziej precyzyjne wytyczne dla radców prawnych jest art. 23 KERP, zgodnie którym:

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.

40. Powołany przepis wprost wskazuje na następujące zabezpieczenia, które trzeba uwzględnić przy przechowywaniu dokumentów w formie elektronicznej:

1) kontrola dostępu;

2) zabezpieczenie systemu przed zakłóceniem działania;

3) zabezpieczenie systemu przed uzyskaniem nieuprawnionego dostępu;

4) zabezpieczenie systemu przed utratą danych.

41. Jak się zauważa: „dokonując zabezpieczenia, radca prawny powinien dochować należytej staranności w tym zakresie. Jest więc obowiązany zabezpieczyć informacje objęte tajemnicą zawodową w sposób, który uwzględni standard powszechnie przyjęty w tego typu działaniach, ich profesjonalny charakter oraz doświadczenie życiowe."[93]

42. W przypadku korzystania z usług zewnętrznych dostawców trudniej ocenić, czy spełniony jest wymóg kontroli dostępu. Radca prawny nie wie przecież kto konkretnie może mieć wgląd w jego dane, a co więcej może nie znać precyzyjnie lokalizacji gdzie dane są przechowywane (może otrzymać np. jedynie komunikat, że jest to na terenie UE). Niektórzy dostawcy przewidują jednak rozwiązania pozwalające na ustalenie czy ktoś uzyskiwał dostęp do danych. Pełna kontrola dostępu, jeśli rozumieć ją w ten sposób, że to radca z góry decyduje kto może mieć wgląd w dane, w standardowych usługach cloudowych będzie jednak bardzo trudna do uzyskania.

[93] T. Jaroszyński, A. Sękowska, P. Skuczyński, *Kodeks Etyki Radcy Prawnego. Komentarz*, Wydawnictwo Praktyka Prawnicza, 2016, str. 122.

43. Jeżeli zaś chodzi o zabezpieczenie systemu przed zakłóceniem działania, uzyskaniem nieuprawnionego dostępu i utratą danych, to jak się przekonamy, gwarancje części usługodawców są w tym zakresie daleko idące i w ich przypadku nie powinno być kontrowersyjnym przyjęcie, że warunki te są spełnione. W praktyce zabezpieczenia gwarantowane przez te podmioty mogą być na poziomie, który trudno uzyskać w niewielkiej kancelarii – przynajmniej bez ponoszenia większych kosztów.

44. Dyskusja na temat zgodności korzystania z usług chmurowych z zasadami etyki nie jest w środowisku prawników nowa.

45. Już w 2012 r. Rada Adwokatur i Stowarzyszeń Prawniczych Europy [„CCBE"] wydała dokument, który zawierał wytyczne dotyczące korzystania przez prawników z chmury.[94] CCBE nie wykluczyła możliwości korzystania przez prawników z chmury publicznej, ale określiła bardzo szeroki krąg okoliczności, które powinien wziąć pod uwagę prawnik decydujący się na korzystanie z takiej usługi. Znaczna część wytycznych Rady dotyczy elementów umownych, które w przypadku dużych dostawców chmur publicznych nie mogą być negocjowane, więc będą niemożliwe do spełnienia (np. kary umowne dla dostawcy czy dostarczenie kodu źródłowego w sytuacji niewypłacalności dostawcy). Przy okazji, warto wspomnieć, że CCBE wydała również praktyczne wskazówki w zakresie poprawy bezpieczeństwa teleinformatycznego prawników przed bezprawnym nadzorem. Nie dotyczą one ściśle przechowywania plików w chmurze, ale warto się z nimi zapoznać.[95]

46. Szereg amerykańskich organizacji prawniczych (np. New York State Bar Association) również wydało opinie dopuszczające możliwość korzystania z chmury przez amerykańskich prawników. W opiniach tych w zasadzie zgodnie podkreśla się, że korzystanie z chmury jest dopuszczalne, ale wymaga podjęcia rozsądnych kroków mających na celu ochronę informacji poufnych.[96]

13. [RODO – przetwarzanie danych]

47. Jak już wspomnieliśmy, w chmurze standardowo dochodzić będzie do przetwarzania danych osobowych. Kancelaria korzystająca z takiej usługi będzie administratorem danych osobowych, a dostawca podmiotem przetwarzającym (co do zasady).

---

[94] *Wytyczne Rady Adwokatur i Stowarzyszeń Prawniczych Europy w Zakresie Korzystania przez Prawników z Usług Pracy w Chmurze*, https://kirp.pl/wp-content/uploads/2017/08/2012-09-07-wytyczne-ccbe-w-zakresie-korzystania-przez-prawnikow-z-uslug-pracy-w-chmurze.pdf, dostęp na dzień 8 lipca 2020 r.

[95] *Praktyczne Wskazówki Rady Adwokatur i Stowarzyszeń Prawniczych Europy w Zakresie Poprawy Bezpieczeństwa Teleinformatycznego Prawników przed Bezprawnym Nadzorem,* https://www.oirpwarszawa.pl/wp-content/uploads/2017/08/Praktyczne-wskazówki-CCBE-w-zakresie-poprawy-bezpieczeństwa-teleinformatycznego-prawników.pdf, dostęp na dzień 8 lipca 2020 r.

[96] Zob. np. New York State Bar Association Ethics Opinion 842, https://nysba.org/ethics-opinion-842/, dostęp na dzień 8 lipca 2020 r.; The Professional Ethics Committee For The State Bar Of Texas Opinion No. 680, https://www.legalethicstexas.com/getattachment/4bad0ccd-9157-4d3f-b14c-0a7fe2ac05f6/Opinion-680, dostęp na dzień 8 lipca 2020 r.

48. Postanowienia RODO nakładają na administratora 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).

49. Radca prawny będący administratorem musi odpowiednio pouczyć osoby, których dane przetwarza o sposobie tego przetwarzania (art. 13 RODO). Pouczenie to powinno uwzględniać kwestię korzystania z chmury, chociażby przez wskazanie dostawcy usługi (jako odbiorcy danych) i zamieszczenie informacji na temat tego, czy dane są przekazywane poza Europejski Obszar Gospodarczy. Radca prawny musi zatem ustalić m.in. gdzie przechowuje dane osobowe podmiot, z usług którego korzysta i czy dokonuje on eksportu danych poza EOG (a jeśli tak, to na jakiej podstawie). W razie potrzeby należy zmodyfikować dotychczas stosowane pouczenie.

50. RODO nakłada na administratorów obowiązek korzystania wyłącznie z 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). Wiarygodność globalnych dostawców usług będzie oparta w części na subiektywnych opiniach oceniającego, jednak można (i należy) wziąć pod uwagę również publikowane przez dostawców materiały i dokumenty oraz informacje o dotychczasowych naruszeniach ochrony danych osobowych, które miały miejsce u tego dostawcy.

51. W związku z tym, że przy korzystaniu z usług cloudowych dochodzi do powierzenia przetwarzania danych, to z dostawcą należy zawrzeć umowę powierzenia przetwarzania danych. W przypadku chmury publicznej oferującej zestandaryzowaną usługę, w praktyce niemożliwe będzie zawarcie indywidualnie negocjowanej umowy powierzenia przetwarzania danych. Mamy tu do czynienia z wzorcami umownymi, które akceptuje się przy zakładaniu konta i których nie można zmienić.

52. Umowa powierzenia przetwarzania danych musi spełniać określone w RODO warunki. Do warunków tych będziemy jeszcze wielokrotnie wracać, zatem warto przywołać w całości przepis, który je wprowadza. Zgodnie z art. 28 ust. 3 RODO:

Przetwarzanie przez podmiot przetwarzający odbywa się 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:

a) *przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji*

międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

b) *zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;*

c) *podejmuje wszelkie środki wymagane na mocy art. 32;*

d) *przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4;*

e) *biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;*

f) *uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36;*

g) *po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;*

h) *udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.*

53. Zgodnie z art. 28 ust. 2 RODO, do którego odwołanie znajduje się w art. 28 ust. 3 lit. d RODO:

Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

54. Artykuł 28 ust. 3 lit. d RODO odwołuje się również do ustępu 4 art. 28 RODO. Zgodnie z tym przepisem:

Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. […].

55. Przed rozpoczęciem korzystania z konkretnej usługi należy zatem zweryfikować umowę powierzenia przetwarzania danych pod kątem tego, czy zawiera wszystkie określone wyżej elementy.

14. [RODO – Schrems II]

56. Oprócz kwestii związanych umową powierzenia przetwarzania danych, drugim kluczowym zagadnieniem z punktu widzenia ochrony danych osobowych, jest przekazywanie danych poza Europejski Obszar Gospodarczy. Może się bowiem zdarzyć, że radca prawny będzie korzystał z usług podmiotu przetwarzającego, który przetwarza powierzone mu dane poza EOG (np. z uwagi na to, że ma siedzibę lub infrastrukturę w państwie trzecim). W praktyce, w przypadku usług chmurowych, największe znaczenie ma transfer danych do USA.

57. Choć RODO nie wprowadziło bezwzględnego nakazu przetwarzania danych osobowych na terenie Unii Europejskiej, to przekazanie danych do państwa trzeciego jest możliwe jedynie w przypadku, gdy spełnione są określone warunki.

58. Jedną z podstaw przekazania danych osobowych do państwa trzeciego jest stwierdzenie przez Komisję Europejską, że to państwo zapewnia odpowiedni stopień ochrony (art. 45 RODO).

59. 12 lipca 2016 r. Komisja Europejska przyjęła decyzję wykonawczą 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA. Komisja uznała, że Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z UE do podmiotów w USA, które są uczestnikami Tarczy Prywatności. Decyzja ta umożliwiała więc przekazywanie danych osobowych przedsiębiorstwom z USA – ale tylko takim, które przystąpiły do tego programu. W programie brało udział około 5 tysięcy uczestników, w tym najwięksi dostawcy usług internetowych (m.in poczty elektronicznej i chmury). Była to więc istotna podstawa umożliwiająca podmiotom ze Stanów Zjednoczonych świadczenie usług na rzecz podmiotów z Unii Europejskiej.

60. Inną podstawą przekazania danych osobowych do państwa trzeciego mogą być tzw. standardowe klauzule ochrony danych (standardowe klauzule umowne).

61. W razie braku decyzji Komisji stwierdzającej, że dane państwo zapewnia odpowiedni stopień ochrony, dane osobowe mogą być przekazywane do takiego państwa wyłącznie gdy: zostaną zapewnione odpowiednie zabezpieczenia, obowiązują egzekwowalne prawa osób, których dane dotyczą i obowiązują skuteczne środki ochrony prawnej (zob. art. 46 RODO). Odpowiednie zabezpieczenie można zapewnić m.in. właśnie przez stosowanie standardowych klauzul ochrony danych przyjętych przez Komisję Europejską (art. 46 ust. 2 lit. c RODO). Są to postanowienia ustalone przez Komisję, które mogą zostać zawarte w umowie między stronami i które mogą stanowić podstawę przekazania danych do państwa trzeciego.

62. Obie wspomniane podstawy przekazywania danych poza EOG były przedmiotem zainteresowania Trybunału Sprawiedliwości Unii Europejskiej w ramach wspomnianego na początku opracowania wyroku ws. Schrems II[97]. W tym konkretnym przypadku Trybunał zajmował się transferem danych do USA.

63. Po pierwsze TSUE uznał, że decyzja wykonawcza Komisji 2016/1250 z dnia 12 lipca 2016 r. w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA jest nieważna.

64. TUSE zwrócił uwagę, że Stany Zjednoczone posiadają wewnętrzne regulacje dotyczące dostępu amerykańskich władz do danych przekazywanych z UE do USA, w szczególności w związku z bezpieczeństwem narodowym USA. Zdaniem TSUE amerykańskie przepisy nie zawierają ograniczeń w dostępie do danych w sposób odpowiadający wymogom ustanowionym w prawie unijnym. TSUE uznał również, że amerykańskie przepisy nie przyznają osobom, których dane są przetwarzane praw, które mogłyby być egzekwowalne przed sądami.

65. W konsekwencji TSUE uznał, że Komisja nieprawidłowo ustaliła, iż Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych przekazywanych z UE i orzekł, że wspomniana decyzja Komisji jest nieważna.

66. Okoliczność, że konkretne przedsiębiorstwo z USA jest uczestnikiem Tarczy Prywatności przestała być więc podstawą umożliwiającą przekazywanie danych osobowych do Stanów Zjednoczonych.

67. W konsekwencji przedsiębiorstwa opierające transfer o ten program straciły podstawę prawną do przekazywania danych do Stanów Zjednoczonych i muszą poszukać innej podstawy lub zaprzestać dokonywania transferu.

[97] Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 16 lipca 2020 r. w sprawie C-311/18.

68. Po drugie TUSE odniósł się do standardowych klauzul umownych. W tym przypadku uznał, że decyzja Komisji[98] określająca te klauzule jest ważna. Przedstawiona przez TSUE w wyroku argumentacja dotycząca wewnętrznych przepisów USA sprawiła jednak, że dopuszczalność transferu danych osobowych do USA w oparciu o standardowe klauzule budzi bardzo duże wątpliwości.

69. Trybunał zwrócił uwagę, że zgodnie z art. 46 ust. 1 RODO, w przypadku przekazywania danych do państwa trzeciego powinny zostać zapewnione odpowiednie zabezpieczenia, egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej. Podmiot przekazujący dane i podmiot odbierający dane mają obowiązek weryfikacji czy w praktyce istnieje możliwość zapewnienia ochrony przekazywanych do państwa trzeciego danych w stopniu merytorycznie równoważnym temu, który jest gwarantowany przez prawo unijne. Aby ocenić czy ma to miejsce należy uwzględnić także istotne elementy składające się na system prawny tego państwa.

70. Tymczasem w przywoływanej już części uzasadnienia poświęconej Tarczy Prywatności TSUE jednoznacznie wskazał, że amerykańskie przepisy dotyczące dostępu i wykorzystywania danych przekazanych z UE, nie przewidują ograniczeń odpowiadających wymogom ustanowionym w prawie unijnym. Dodatkowo osobom, których dane zostały przekazane do USA z UE, przepisy amerykańskie nie przyznają egzekwowalnych praw przed sądami.

71. Argumentację tę można bezpośrednio przenieść na ocenę tego, czy w przypadku przekazania danych do USA w oparciu o standardowe klauzule, istnieje możliwość zapewnia odpowiednich zabezpieczeń, egzekwowalnych praw i skutecznych środków ochrony prawnej. Potwierdza to stanowisko Europejskiej Rady Ochrony Danych, która już wskazała, że próg ustalony przez TUSE ma zastosowanie również do przekazywania danych na podstawie art. 46 RODO (czyli m.in. na podstawie standardowych klauzul).[99]

72. Taka ocena amerykańskiego systemu prawnego przez TSUE powoduje, że obecnie dopuszczalność transferu danych do USA stanęła pod dużym znakiem zapytania.

[konsekwencje wyroku TSUE]

73. Po wyroku TSUE znaleźliśmy się więc w stanie dużej niepewności prawnej w zakresie przekazywania danych do Stanów Zjednoczonych.

---

[98] Decyzja Komisji 2010/87/UE z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podwykonawcom mającym siedzibę w państwach trzecich na podstawie dyrektywy Parlamentu Europejskiego i Rady 95/46/WE, zmieniona decyzją wykonawczą Komisji (UE) 2016/2297 z dnia 16 grudnia 2016 r.

[99] *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems,* 23 lipca 2020 r., str. 2, https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf, dostęp na dzień 25 lipca 2020 r.

74. Radcowie prawni powinni zatem przeanalizować wszystkie narzędzia, z których korzystają w kancelarii i ustalić, czy w wyniku korzystania z tych narzędzi dochodzi do przekazania danych do USA. Nie dotyczy to tylko usług przechowywania plików w chmurze, ale także poczty elektronicznej, systemów CRM, czy narzędzi do organizacji pracy.

75. W przypadku gdy zostanie ustalone, że taki transfer ma miejsce, trzeba zweryfikować podstawę prawną w oparciu, o którą się on odbywa. Informacje na ten temat można odnaleźć w umowach powierzenia udostępnianych przez usługodawców i innych dokumentach przez nich publikowanych.

76. Jeżeli usługodawca informuje, że jedyną podstawą przekazywania danych do USA było jego uczestnictwo w Tarczy Prywatności, to taki transfer danych bez wątpienia trzeba zatrzymać. Przekazywanie danych na tej podstawie nie jest już bowiem legalne.

77. Jednak nawet jeśli Tarcza Prywatności nie była jedyną podstawą przekazywania danych a usługodawca wykorzystywał (obok lub zamiast Tarczy) standardowe klauzule umowne, to dalsze korzystanie z usług takiego podmiotu może budzić wątpliwości z uwagi na kwestie dotyczące istoty systemu ochrony danych w USA, o których wspomnieliśmy wyżej.

78. Europejska Rada Ochrony Danych wskazała, że możliwość dalszego przekazywania danych do USA na podstawie standardowych klauzul zależy od indywidualnie dokonanej oceny. Pod uwagę należy wziąć okoliczności transferu i dodatkowe środki uzupełniające, które można zastosować. Zdaniem EROD, jeżeli zastosowanie odpowiednich zabezpieczeń nie będzie możliwe, to wymagane jest zawieszenie lub zakończenie przekazywania danych osobowych.[100]

79. Prezes Urzędu Ochrony Danych Osobowych potwierdził, że administratorzy danych muszą dokonać „indywidualnej oceny stopnia ochrony danych zapewnianego w ramach takiego transgranicznego przekazywania danych, która musi uwzględniać nie tylko same postanowienia umowne uzgodnione między eksporterami i importerami danych, lecz również przepisy prawa w państwie trzecim, w szczególności odnoszące się do ewentualnego dostępu organów władzy publicznej tego państwa do przekazywanych danych. Gdy w świetle dokonanej oceny poziom ochrony danych osobowych nie będzie merytorycznie równoważny z poziomem gwarantowanym w UE, przekazywanie danych może być uzależnione od zapewnienia równoważnego poziomu ich ochrony za pomocą innych środków."[101]

80. Powyższe uwagi dotyczą oczywiście również usług chmurowych. Część dostawców takich usług ma bowiem siedzibę w Stanach Zjednoczonych i tam przetwarza dane zamieszczone przez użytkowników

---

[100] *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems,* 23 lipca 2020 r., str.3, https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf, dostęp na dzień 25 lipca 2020 r.

[101] Komunikat zamieszczona na stronie www.uodo.gov.pl, *Wyrok TSUE ws. Data Protection Commissioner przeciwko Facebook Ireland Ltd. i Maximilian Schrems*, https://uodo.gov.pl/pl/138/1603, dostęp na dzień 25 lipca 2020 r.

(w tym radców prawnych). Inni z kolei mają siedzibę w Unii Europejskiej, lecz są to spółki zależne podmiotów amerykańskich i część danych przekazują do Stanów Zjednoczonych. Kwestia lokalizacji przetwarzania danych osobowych – już wcześniej istotna – teraz nabiera kluczowego znaczenia.

81. Radca prawny, który ustali, że korzysta z usług podmiotu przekazującego dane do USA na podstawie standardowych klauzul umownych, musi więc ocenić ryzyko dalszego korzystania z tego narzędzia. Może ewentualnie poszukać innej podstawy transferu danych do USA (art. 49 RODO). Jeśli to możliwe to powinien tak skonfigurować usługę, żeby w dane były przetwarzane tylko na obszarze EOG.

82. W naszej ocenie – na ten moment – wydaje się, że przekazywanie danych do USA na podstawie standardowych klauzul zostanie zakwestionowane. Sytuacja jest co prawda dynamiczna, jednak argumentacja TSUE spowodowała, że transfer danych do Stanów Zjednoczonych na podstawie klauzul (bez stosowania dodatkowych środków bezpieczeństwa), jest co najmniej bardzo problematyczny. Stosowanie zaś dodatkowych zabezpieczeń w standardowych usługach chmurowych na ten moment wydaje się być poza zasięgiem użytkowników. Musiałyby one bowiem zostać wdrożone przez dostawcę. Być może w przypadku usług chmurowych, skutecznym środkiem, którego stosowanie leży po stronie użytkownika, byłoby stosowanie szyfrowania end-to-end plików przekazywanych do chmury. Dostawca usługi nie miałby bowiem wglądu do tak zaszyfrowanych danych.

83. M. Gawroński wskazał (choć zaznaczył, że jest to ocena wstępna), że jego zdaniem dopuszczalne powinno być korzystanie z usług „w których transfer danych do USA nie dotyczy tzw. kontentu (user generated content)", a „transferowane są dane telemetryczne a nawet dane podstawowe użytkowników (jednolita książka adresowa)."[102] Jak się przekonamy kwestia ta w praktyce może mieć istotne znaczenie dla niektórych dostawców.

84. W przypadku braku zastosowania dodatkowych zabezpieczeń (np. szyfrowania w pełni zabezpieczającego dane przed dostępem), radca prawny, który chce uniknąć jakiegokolwiek ryzyka powinien rozważyć rezygnację z przekazywania danych osobowych do Stanów Zjednoczonych. Przynajmniej do czasu kiedy wątpliwe kwestie nie zostaną przesądzone przez organy nadzoru. Zachęcamy do uważnego obserwowania sytuacji i publikowanych stanowisk związanych z przekazywaniem danych do USA.

[102] M. Gawroński, *Co dalej z usługami chmurowymi po wczorajszym wyroku TSUE?,* 17 lipca 2020 r., https://www.linkedin.com/pulse/co-dalej-z-us%25C5%2582ugami-chmurowymi-po-wczorajszym-wyroku-maciej/?trackingId=VgHAqWDIFncAUiuyLkv%2FrQ%3D%3D, dostęp na dzień 25 lipca 2020 r.

V. SZYFROWANIE DANYCH W CHMURZE

15. [informacje wstępne]

85. Jednym z kluczowym elementów związanych z bezpieczeństwem chmury jest szyfrowanie przechowywanych w niej danych.

86. W związku z tym, że stosowane metody szyfrowania wpływają na bezpieczeństwo przechowywanych danych, w niniejszym opracowaniu omówimy deklaracje dostawców dotyczące tego jak szyfrują oni dane usługobiorców. Aby dalsza część opinii była bardziej zrozumiała przedstawimy poniżej podstawowe informacje dotyczące szyfrowania, jednak oczywiście nie aspirujemy do pełnego wyjaśnienia tej problematyki.

87. Choć szyfrowanie jest zagadnieniem, którego pełne zrozumienie wymaga posiadania specjalistycznej wiedzy, to w naszej ocenie warto zapoznać się przynajmniej z podstawowymi pojęciami dotyczącymi tej problematyki.

88. W publikacjach dotyczących szyfrowania wskazuje się, że sprawia, ono 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."[103]

89. Istnieje wiele metod i rodzajów szyfrowania (np. szyfrowanie asymetryczne i symetryczne), jednak na potrzeby tej informacji najważniejsze będzie wyróżnienie dwóch zastosowań szyfrowania:

1) szyfrowanie danych „w spoczynku" („at-rest encryption") oraz

2) szyfrowanie danych „w trakcie przesyłu" („in transit encryption").

16. [szyfrowanie „w spoczynku"]

90. W szyfrowaniu „w spoczynku" chodzi o zabezpieczenie danych w momencie kiedy nie są używane i są przechowywane (np. na serwerach). Istota korzystania z chmury publicznej polega na umieszczeniu plików na serwerach dostawcy. Są one przechowywane na tych serwerach nie tylko w momencie, w którym użytkownik je otwiera, ale przez cały czas. Szyfrowanie danych „w spoczynku" będzie więc odgrywało kluczową rolę w przypadku chmury, ponieważ pozwala zabezpieczyć dane, które są permanentnie trzymane w zewnętrznej infrastrukturze.

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

91. Jak się przekonamy, wszyscy dostawcy, których usługi przeanalizowaliśmy deklarują szyfrowanie danych „w spoczynku". Takie szyfrowanie chroni dane przed nieuprawnionym dostępem osób z zewnątrz, co jednak kluczowe dla zrozumienia działania chmury, nie oznacza ono, że do danych nie ma dostępu usługodawca. Standardowo to dostawca usługi szyfruje dane przechowywane w chmurze i to on dysponuje kluczami umożliwiającymi zdeszyfrowanie tych danych. To zaś prowadzi do wniosku, że dostawca dysponował będzie (przynajmniej potencjalną) możliwością zapoznania się z danymi.

92. Oczywiście dla części radców prawnych nawet potencjalna możliwość zapoznania się z danymi przez podmiot trzeci może powodować obawę przed korzystaniem z chmury, z uwagi na wątpliwość, czy nie dochodzi wówczas do naruszenia tajemnicy zawodowej.

93. Tacy radcowie nie muszą być jednak skazani na przechowywanie plików lokalnie lub na własnych serwerach. Istnieją bowiem chmury, w których dostawca nie będzie mógł zapoznać się z przechowanymi plikami. Taka sytuacja ma miejsce w przypadku gdy wspierane jest pełne szyfrowanie (tzw. „zero-knowledge encryption"). W przypadku standardowych wersji chmur publicznych, które przeanalizowaliśmy takie szyfrowanie nie jest jednak dostępne.

94. Można również korzystać z narzędzi umożliwiających szyfrowanie danych na urządzeniu użytkownika i przesłać pliki do chmury publicznej w formie już zaszyfrowanej. Dostawca chmury nie będzie dysponował kluczem umożliwiającym odszyfrowanie tych plików, więc nie będzie mógł się zapoznać z ich treścią. Dane są wtedy dodatkowo zabezpieczone. Takie rozwiązania są również dostarczane przez polskich przedsiębiorców. Radcowie, którzy chcieliby ograniczyć ryzyko naruszenia tajemnicy zawodowej lub przechowują szczególnie istotne dokumenty powinni rozważyć ich zastosowanie.

17. [szyfrowanie „w trakcie przesyłu"]

95. Z kolei szyfrowanie „w trakcie przesyłu" ma na celu zabezpieczenie danych w momencie, w którym następuje ich transfer. W przypadku chmury, szyfrowanie „w trakcie przesyłu" chroni dane m.in. w momencie ich przesyłania z urządzenia usługobiorcy do chmury i z chmury do urządzenia usługobiorcy, a także przy przesyłaniu danych między różnymi serwerami usługodawcy.

96. W powołanej już publikacji dotyczącej kryptografii tak podsumowano oba zastosowania szyfrowania: „Szyfrowanie podczas transferu (in-transit encryption) chroni dane wysyłane z jednej maszyny do drugiej: dane są szyfrowane przed wysłaniem i odszyfrowywane po ich odebraniu jak w szyfrowanych połączeniach witryn e-handlu. Szyfrowanie w spoczynku (at-rest encryption) chroni dane przechowywane w systemie informacyjnym. Dane są szyfrowane przed ich zapisaniem w pamięci i odszyfrowywane przed ich odczytaniem. Wśród przykładów są systemy szyfrowania dysku na laptopach, a także szyfrowanie maszyn wirtualnych dla wirtualnych instancji w chmurze."[104]

[104] Jean-Philippe Aumasson, *Nowoczesna kryptografia,* Wydawnictwo Naukowe PWN, 2018, str. 43.

97. Ochronie danych „w trakcie przesyłu" służy protokół o nazwie Transport Layer Security (TLS). Pierwotnie był on znany jako SSL i taką nazwę można często spotkać w praktyce. Protokół SSL został opracowany w połowie lat dziewięćdziesiątych, a następnie w roku 1999 został zastąpiony protokołem TLS 1.0. W kolejnych latach powstawały kolejne, coraz bardziej rozbudowane protokoły – TLS 1.1 (2006 r.), TLS 1.2 (2008 r.) i wreszcie TLS 1.3 (2018 r.). Przy omawianiu szyfrowania „w trakcie przesyłu" zapewnianego przez poszczególnych dostawców wskażemy jakie wersje TLS wspierają dostawcy.

98. Działanie protokołu TLS jest opisywane w następujący sposób: „TLS jest najbardziej znany jako litera S w witrynach HTTPS oraz kłódka w pasku adresu przeglądarki, które wskazują, że strona jest bezpieczna. Podstawową motywacją utworzenia TLS było umożliwienie bezpiecznego przeglądania w aplikacjach, takich jak e-handel lub e-banki, przez szyfrowanie połączeń z witryną, aby chronić numery kart kredytowych, poświadczenia użytkownika oraz inne wrażliwe informacje. TLS pomaga także w ogólnej ochronie połączeń internetowych przez ustanowienie bezpiecznego kanału między klientem a serwerem, który zapewnia poufność, uwierzytelnienie i niezmienność transferu danych. Jednym z celów bezpieczeństwa TLS jest zapobieganie atakom typu man-in-the-middle, 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 […]."[105]

99. Protokół ten zabezpiecza więc połączenie między użytkownikiem a serwerami, ale nie chroni danych samych w sobie.[106] TLS szyfruje połączenie, a nie bezpośrednio treść wiadomości. W przypadku wiadomości e-mail szyfrowanie „w trakcie przesyłu" zabezpiecza ruch pomiędzy nadawcą wiadomości, serwerami poczty oraz odbiorcą. Przy usługach chmurowych zabezpieczany będzie ruch pomiędzy stacją roboczą użytkownika a serwerami dostawcy usługi oraz ewentualnie pomiędzy serwerami dostawcy. Warunkiem jest jednak by użytkownik korzystał z oprogramowania (np. przeglądarki internetowej), która wspiera ten rodzaj szyfrowania.

VI. GOOGLE DRIVE (DYSK GOOGLE)

18. [informacje wstępne]

100. Google Drive jest chmurową usługą do przechowywania i synchronizacji plików. Jest częścią popularnego pakietu G Suite.

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

101. Dostawcą usług wchodzących w skład G Suite dla klientów z Europejskiego Obszaru Gospodarczego jest Google Ireland Limited z siedzibą w Dublinie (Irlandia). Umowa zawierana z Google podlega prawu angielskiemu.[107]

102. Aplikację można zainstalować zarówno na komputerach z systemem Windows jak i systemem macOS. Działa również na urządzeniach mobilnych (w tym z systemem Android i iOS), co pozwala na łatwy dostęp do plików także w sytuacji gdy nie mamy przy sobie komputera.

103. Istnieje również darmowa wersja tej usługi. W naszej ocenie możliwość korzystania z darmowej wersji w działalności zawodowej radców prawnych budzi jednak wątpliwości. Co ciekawe, jeszcze w latach 2018-19 w „Warunkach korzystania z Dysku Google" znajdowało się postanowienie, zgodnie z którym użytkownik akceptując warunki zgadzał się „nie używać Dysku Google w celach komercyjnych".[108] Zwracaliśmy wówczas uwagę, że takie postanowienie powoduje, że darmowa wersja Google Drive nie powinna być wykorzystywana w działalności zawodowej radców prawnych i powinni oni korzystać z płatnej wersji, będącej częścią pakietu G Suite.

104. W obecnie obowiązujących warunkach takie ograniczenie się nie znalazło.[109] W dalszym ciągu mamy jednak pewne wątpliwości co do korzystania z darmowej wersji tej usługi przez radców prawnych. Powodem jest treść dokumentu pod nazwą „Warunki korzystania z usług Google".[110]

105. Zgodnie z tymi warunkami korzystania z usług Google, użytkownik udziela Google licencji na korzystanie z treści przesyłanych, przechowywanych, czy wysyłanych przy użyciu usług Google, a licencja obejmuje możliwość używania automatycznych systemów i algorytmów do analizowania treści użytkownika m.in. pod kątem spamu, także po to by dostosować usługi Google do użytkownika, w tym przedstawiać rekomendacje i spersonalizowane wyniki wyszukiwania, treści oraz reklamy.[111] Gdyby znaczyło to, że pliki radcy prawnego zawierające informacje objęte tajemnicą radcowską są skanowane w celu dopasowania reklam, to musiałoby to wzbudzić niepokój.

106. Co ciekawe przywołane wyżej warunki zostały opracowane w taki sposób, że wydają się mieć zastosowanie zarówno do usług bezpłatnych jak i płatnych. Przy zakładaniu konta G Suite użytkownik akceptuje jednak umowę dotyczącą tego pakietu [„G Suite Agreement"], w której takiego uprawnienia

---

[107] *G Suite Agreement*, https://admin.google.com/terms/apps/1/11/en/premier_terms_eea.html, dostęp na dzień 8 lipca 2020 r.
[108] *Warunki korzystania z Dysku Google z 22 stycznia 2019 r.* (archiwalne), https://www.google.com/intl/pl/drive/terms-of-service/archived/, dostęp na dzień 8 lipca 2020 r.
[109] *Dodatkowe warunki korzystania z usługi Dysk Google z 31 marca 2020 r.,* https://www.google.com/drive/terms-of-service/, dostęp na dzień 8 lipca 2020 r.
[110] *Warunki korzystania z usług Google z 31 marca 2020 r.*, https://policies.google.com/terms?hl=pl, dostęp na dzień 8 lipca 2020 r.
[111] *Warunki korzystania z usług Google z 31 marca 2020 r.*, https://policies.google.com/terms?hl=pl, dostęp na dzień 8 lipca 2020 r.

dla Google nie przewidziano.[112] W umowie tej znajdują się też daleko idące postanowienia dotyczące poufności.

107. Wydaje się zatem, że w przypadku pakietu G Suite, Google nie analizuje treści użytkownika w celu targetowania reklam. W obecnie obowiązujących „Dodatkowych warunkach korzystania z usługi Dysk Google" znajduje się deklaracja Google, zgodnie z którą dostawca nie używa treści użytkownika „na potrzeby marketingu ani kampanii promocyjnych."

108. Poniżej będziemy omawiali płatną wersję Google Drive, która jest częścią pakietu G Suite.

19. [Google Drive a RODO]

109. Google deklaruje oczywiście pełną zgodność swojego działania z przepisami dotyczącymi ochrony danych osobowych (w tym RODO).[113] W umowach podpisywanych z klientami, Google zobowiązuje się do przestrzegania przepisów RODO i oferuje dodatkowe opcje związane z ochroną danych. Dotyczy to również przetwarzania danych w ramach pakietu G Suite (a więc również Google Drive).[114] Na marginesie wskazujemy, że francuski organ nadzoru CNIL nałożył w 2019 r. na spółkę Google LLC karę w wysokości 50 milionów euro m.in. za brak jasnej informacji o zasadach przetwarzania danych użytkowników.

110. Jeśli chodzi o przechowywanie danych, to centra danych Google znajdują się w Europie, Ameryce Północnej, Ameryce Południowej i Azji. Google korzysta z centrów danych znajdujących się w 5 lokalizacjach na terenie Unii Europejskiej. Są to Dublin (Irlandia), Eemshaven (Holandia), Fredericia (Dania) Hamina (Finlandia), St. Ghislain (Belgia).[115]

111. Google wprowadził możliwość wyboru terytorium, na którym mają być przetwarzane dane osobowe użytkownika. Użytkownik pakietu G Suite[116] ma możliwość wybrania lokalizacji geograficznej, w której będą przetwarzane jego dane.[117] Użytkownicy z Polski mogą zatem wybrać, by ich dane były przetwarzane wyłącznie w centrach znajdujących się w Unii Europejskiej. Po wybraniu regionu europejskiego wszystkie dane upload'owane do Dysku Google będą przechowywane w europejskich centrach danych.[118]

---

[112] *G Suite Agreement*, https://admin.google.com/terms/apps/1/11/en/premier_terms_eea.html, dostęp na dzień 8 lipca 2020 r.
[113] Zob. np. https://cloud.google.com/security/gdpr#tab4, dostęp na dzień 8 lipca 2020 r.
[114] Zob. np. https://cloud.google.com/security/gdpr, dostęp na dzień 8 lipca 2020 r., https://cloud.google.com/security/gdpr/resource-center, dostęp na dzień 8 lipca 2020 r.
[115] https://www.google.com/about/datacenters/locations/, dostęp na dzień 8 lipca 2020 r.
[116] Funkcja jest dostępna w następujących pakietach: G Suite Business, G Suite Enterprise, G Suite Enterprise dla Szkół i Uczelni, G Suite Enterprise Essentials.
[117] Zob. *Wybieranie lokalizacji geograficznej na potrzeby przechowywania danych,* https://support.google.com/a/answer/7630496?hl=pl, dostęp na dzień 8 lipca 2020 r.
[118] Potwierdza to zestawienie danych objętych regułami dotyczącymi lokalizacji przechowywanych danych dostępne pod tym linkiem https://support.google.com/a/answer/9223653?visit_id=637292923071011602-2254762998&rd=1, dostęp na dzień 8 lipca 2020 r.

112. Co ciekawe, już w poprzednim roku, Google zapowiedziało, że uruchomi centrum danych dla usług chmurowych w Polsce. Centrum ma zostać otwarte w 2021 r.[119] Być może pojawi się więc opcja wyboru by dane były przechowywane konkretnie w centrum danych znajdującym się w Polsce.

113. W dodatku nr 2 do umowy powierzenia przetwarzania danych zawieranej z Google [„DPA"][120] wskazano, że Google przechowuje dane użytkownika w wielu geograficznie rozproszonych centrach danych, chyba że użytkownik wydał instrukcję co do lokalizacji danych. Można to więc traktować jako umowne zobowiązane Google do przetwarzania danych w obszarze faktycznie określonym przez użytkownika.

114. Co ciekawe jednak, nawet w przypadku wyboru europejskich centrów danych jako lokalizacji, w których mają być przetwarzane dane osobowe, „zasad dotyczących regionów danych nie można stosować do danych klientów indywidualnych ani innych typów danych (takich jak dzienniki czy informacje z pamięci podręcznej), które nie zostały wymienione" w zestawieniu opracowanym przez Google.[121] Oznacza to, że część informacji może być jednak przekazywana poza EOG. Mamy nadzieję, że Google – w kontekście wyroku w sprawie Schrems II – potwierdzi, że wśród tych informacji nie ma danych osobowych. Obecna informacja jest bowiem zbyt lakoniczna by w pełni to przesądzić, szczególnie w zakresie dotyczącym „informacji z pamięci podręcznej".

115. Google LLC (spółka amerykańska) była uczestnikiem programu Tarcza Prywatności. Oprócz tej podstawy przekazywania danych, Google stosuje standardowe klauzule umowne, o których mowa w art. 46 ust. 2 lit. c RODO.[122]

116. Po wybraniu przez użytkownika aby jego dane były przetwarzane w centrach znajdujących się na terenie Unii Europejskiej i upewnieniu się (ewentualnie potwierdzeniu przez Google), że wśród informacji przekazywanych do spółki amerykańskiej nie ma danych osobowych, korzystanie z tej usługi przez unijnych użytkowników nie powinno budzić wątpliwości w kontekście transferu danych do USA.

117. Co do zasady Google w stosunku do danych użytkownika przechowywanych na Dysku Google pełni rolę podmiotu przetwarzającego w rozumieniu art. 28 RODO.

---

[119] *Google zainwestuje w Polsce 2 mld dolarów, uruchomi centrum obliczeniowe w chmurze*, https://www.wirtualnemedia.pl/artykul/google-zainwestuje-w-polsce-2-mld-dolarow-uruchomi-centrum-obliczeniowe-w-chmurze, dostęp na dzień 8 lipca 2020 r.

[120] Tekst umowy powierzenia przetwarzania danych jest dostępny pod tym linkiem: https://gsuite.google.com/terms/dpa_terms.html?_ga=2.232740575.1516864985.1594028275-543829462.1593618309, dostęp na dzień 8 lipca 2020 r.

[121] Zestawienie to jest dostępne pod tym linkiem: https://support.google.com/a/answer/9223653?visit_id=637292923071011602-2254762998&rd=1, dostęp na dzień 8 lipca 2020 r.

[122] Z treścią Standardowych Klauzul Umownych stosowanych przez Google można zapoznać się pod tym linkiem https://gsuite.google.com/terms/mcc_terms.html?_ga=2.194278125.1516864985.1594028275-543829462.1593618309, dostęp na dzień 8 lipca 2020 r.

118. Rozpoczynając korzystanie z pakietu G Suite, użytkownik zawiera z Google umowę powierzenia przetwarzania danych. Bez uważnej lektury warunków korzystania z usług (G Suite Agreement) można przeoczyć, że dochodzi również do zawarcia DPA. Warunki te zawierają jednak informację, że umowa powierzenia przetwarzania danych jest częścią G Suite Agreement. Trzeba jednak zapoznać się z nią odrębnie. Umowę powierzenia można zaakceptować również z poziomu ustawień administratora.[123] Radców, którzy korzystają z pakietu G Suite zachęcamy do weryfikacji, czy potwierdzili oni zawarcie DPA z Google.

119. Poniżej skrótowo przeanalizujemy, czy DPA proponowana przez Google spełnia warunki wynikające z RODO.

120. W swoim DPA Google zobowiązuje się m.in., że będzie przetwarzało dane osobowe zgodnie z instrukcjami użytkownika wynikającymi z umowy lub udokumentowanymi w formie pisemnej (pkt. 5.2.1 i 5.2.2. DPA). Umowa spełnia więc warunek wskazany w art. 28 ust. 3 lit. a RODO.

121. W DPA wprost wskazano, że Google osoby, które będą upoważnione do przetwarzania danych osobowych użytkownika zostaną zobowiązane do zachowania poufności (pkt 7.1.3 DPA). Umowa spełnia więc warunek wskazany w art. 28 ust. 3 lit. b RODO.

122. Google stosuje środki techniczne i organizacyjne pozwalające chronić dane użytkownika przed zniszczeniem, utratą, zmianą, nieuprawnionym dostępem czy ujawnieniem. Google potwierdza stosowanie szyfrowania danych. Stosowane środki mają również na celu: (i) zapewnienie poufności, integralności, dostępności i odporności systemów i usług, (ii) przywracanie dostępności danych osobowych po incydentach, (iii) testowanie efektywności (pkt 7.1 DPA). Stosowane środki techniczne i organizacyjne zostały opisane szczegółowo w załączniku nr 2 do DPA. Umowa spełnia więc warunek wskazany w art. 28 ust. 3 lit. c RODO.

123. Klient zawierając umowę powierzenia z Google upoważnia dostawcę do korzystania z subprocesorów, czyli podmiotów, którym Google może podpowierzyć przetwarzanie danych (pkt 11.1 DPA). W DPA zamieszczony jest link do listy subprocesorów, z usług których korzysta Google.[124] Lista ta może być aktualizowana przez Google. W przypadku gdy Google zamierza skorzystać z usług nowego podmiotu, to ma obowiązek zawiadomić o tej okoliczności klienta przynajmniej 30 dni przed tym, nim ten podmiot zacznie przetwarzać dane osobowe klienta (pkt 11.4 DPA). Klient ma prawo sprzeciwić się korzystaniu z usług nowego subprocesora w terminie 90 dni od przesłania mu informacji przez Google. Dojdzie jednak wówczas do rozwiązania umowy klienta z Google. Google deklaruje również, że nakłada na subprocesorów obowiązki wynikające z RODO (pkt 11.3 DPA). Wobec takiego ujęcia

[123] Zob. więcej: https://support.google.com/a/answer/2888485?hl=en, dostęp na dzień 8 lipca 2020 r.
[124] *G Suite Agreement and/or Complementary Product Agreement – Subprocessors*, https://gsuite.google.com/intl/en/terms/subprocessors.html, dostęp na dzień 8 lipca 2020 r.

postanowień umowy, w naszej ocenie, spełniony jest warunek, o którym mowa w art. 28 ust. 3 lit. d w zw. art. 28 ust. 2 i 4 RODO.

124. Google pomaga klientom wywiązać się z obowiązków określonych w rozdziale III RODO, które dotyczą odpowiadania na żądania osób, których dane dotyczą (pkt 9.2.2 DPA), co jest zgodne z warunkiem określonym w art. 28 ust. 3 lit. e RODO.

125. W DPA znajduje się również deklaracja, że Google zapewnia użytkownikom wsparcie (Security Assistance) w zapewnieniu zgodności ich działania z: (i) art. 32 – 34 RODO (pkt 7.1.4 DPA) oraz (ii) art. 35 i 36 RODO (pkt 8 DPA). Formalnie czyni to zadość obowiązkowi, o którym mowa w art. 28 ust. 3 lit. f RODO).

126. Po zakończeniu świadczenia usług przez Google, klient zleca dostawcy usunięcie swoich danych (w tym wszystkich kopii) z systemów Google, chyba że prawo Unii lub prawo państwa członkowskiego wymaga przechowywania danych (pkt 6.2 DPA). Trzeba jednak pamiętać, że Google nie musi usunąć wszystkich danych od razu. Zgodnie z DPA ma na to maksymalnie 180 dni (pkt 6.2 DPA). Mimo tego należy uznać warunek z art. 28 ust. 3 lit. g RODO za spełniony.

127. Co ciekawe, Google deklaruje, że zezwala klientom lub niezależnym audytorom na prowadzenie audytów (w tym inspekcji) w celu weryfikacji zgodności działania Google z obowiązkami wynikającymi z DPA (pkt 7.5.2 DPA). Jesteśmy ciekawi jak w praktyce odbywałby się taki audyt z uwagi na skalę działalności dostawcy. Biorąc jednak pod uwagę to zobowiązanie oraz fakt, że Google udostępnia materiały opisujące stosowane zabezpieczenia można uznać, że warunek z art. 28 ust. 3 lit. h RODO jest spełniony.

128. Trzeba również zauważyć, że Google zobowiązuje się do niezwłocznego informowania klientów o incydentach związanych z danymi osobowymi (pkt 7.2.1 DPA).

129. Google podkreśla, że posiada certyfikaty takie jak: ISO/IEC 27001 (Zarządzanie Bezpieczeństwem Informacji), ISO/IEC 27017 (Bezpieczeństwo w Chmurze), ISO/IEC 27018 (Ochrona Danych Osobowych w Chmurze).[125]

130. Jak wskazywaliśmy wcześniej, z art. 28 ust. 1 RODO wynika, że radcowie prawni korzystając z usług procesorów powinni wybierać takie podmioty, które zapewniają „wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi" RODO i chroniło prawa osób, których dane dotyczą. W naszej ocenie, biorąc pod uwagę treść umowy powierzenia przetwarzania danych oraz treść dokumentów publikowanych przez Google nie ma powodów by twierdzić, że korzystanie z pakietu G Suite jest niezgodne z RODO, choć należy uważnie

[125] Zob. więcej Google Cloud Whitepaper, *General Data Protection Regulation (GDPR),* maj 2018 r., https://cloud.google.com/security/gdpr/resource-center/pdf/googlecloud_gdpr_whitepaper_618.pdf, dostęp na dzień 8 lipca 2020 r.

przyglądać się kwestii wyjaśnień w zakresie tego jakie konkretnie dane (i czy w ogóle) Google przekazuje poza EOG.

20. [szyfrowanie w Google Drive]

131. Google publikuje na swoich stronach internetowych wiele informacji na temat zasad, w oparciu o które szyfruje dane użytkowników G Suite. Informacje te przeanalizowaliśmy pod kątem szyfrowania plików w Google Drive.

132. W przypadku Google Drive szyfrowane „w spoczynku" są pliki przesłane do chmury przez aplikację zainstalowaną na komputerze (zarówno w przypadku systemów Windows jak i macOS), przeglądarkę internetową, czy przez pocztę Gmail. Co ciekawe Google wprost informuje, że jeśli przesyłanym plikiem jest plik wideo to może nie być on szyfrowany. Dostawca nie podaje jednak powodów z powodu których nie szyfruje plików wideo. [126]

133. Szyfrowanie danych „w spoczynku" odbywa się w sposób automatyczny tzn. użytkownik nie musi wykonywać żadnych działań w celu jego uruchomienia. Szyfrowanie odbywa się w momencie zapisu na dysku i obejmuje również kopie zapasowe danych.

134. 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.[127]

135. Oznacza to, że nie mamy tu do czynienia z „zero-knowledge encryption", jednak Google przedstawia deklaracje, że nawet potencjalny dostęp do danych przechowywanych w ich chmurze będzie ograniczony. Deklaracje te są opisane szerzej w dokumencie „Google Cloud whitepapper Trusting your data with G Suite".[128] 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 deklaruje, że ogranicza liczbę pracowników mających dostęp do danych użytkowników i aktywnie monitoruje aktywność tych pracowników.

---

[126] *G Suite Encryption Whitepaper*, https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf, str. 4, dostęp na dzień 8 lipca 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.

[127] *G Suite Encryption Whitepaper*, https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf, str. 3, dostęp na dzień 8 lipca 2020 r.

[128] *Google Cloud whitepapper*, https://cloud.google.com/files/gsuite-trust-whitepaper.pdf, grudzień 2019, str. 10-11, dostęp na dzień 8 lipca 2020 r.

136. Google 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).[129]

137. Google deklaruje również stosowanie szyfrowania „w trakcie przesyłu", czyli w momencie przesyłania danych od użytkownika na serwery Google oraz między centrami danych Google.

138. W przypadku szyfrowania „w trakcie przesyłu" – jak już wspomniano – konieczne jest by użytkownik korzystał z oprogramowania wspierającego to szyfrowanie. Zwraca na to uwagę Google wskazując, że użytkownik powinien korzystać z bezpiecznej przeglądarki wspierającej szyfrowanie. W przypadku klientów G Suite, dostawca automatycznie szyfruje transmisję pomiędzy przeglądarką użytkownika i swoimi centrami danych. Google korzysta m.in. z algorytmu kryptograficznego z kluczem publicznym RSA (2048-bitowy).[130]

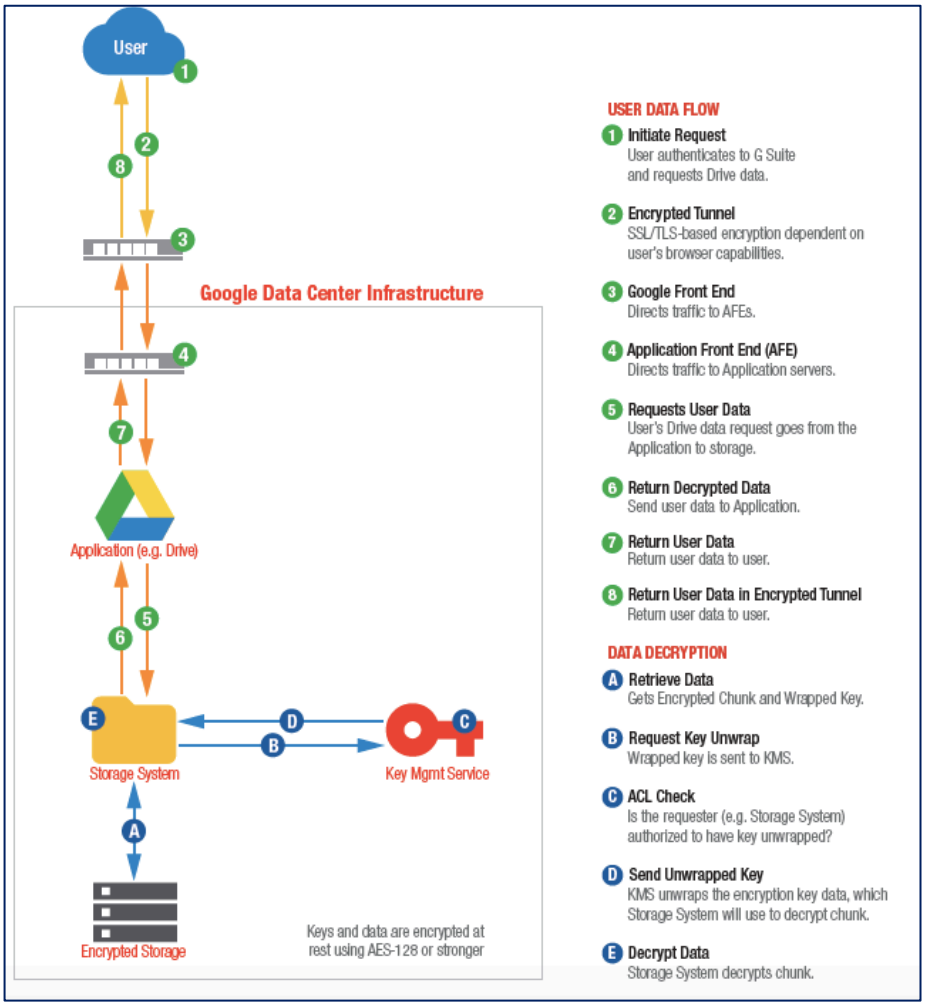
139. Dane mogą być przekazywane nie tylko między stacją roboczą użytkownika a serwerem Google, ale również pomiędzy centrami danych (data centers) Google. Dostawca deklaruje, że dane przenoszone pomiędzy centrami danych są zawsze zaszyfrowane. Zaszyfrowane jest również wewnętrzne połączenie pomiędzy serwerami Google. Według Google niektóre połączenia są zaszyfrowane protokołem „podobnym" do TLS, który używa szyfru AES 128-bitowego lub wyższego.[131]

140. 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.

141. Poniższa grafika opracowana przez Google obrazuje schemat szyfrowania w przypadku Google Drive. W tym schemacie użytkownik (User) oznaczony niżej numerem 1 rozpoczyna łączenie z Google Drive. Połączenie to jest szyfrowane protokołem TLS (numer 2), o ile oczywiście sprzęt użytkownika obsługuje ten protokół. Żądanie użytkownika jest następnie przetwarzane wewnętrznie przez Google, co obrazują grafiki opatrzone numerami 3, 4 i 5. Żądanie przechodzi przez aplikację – w tym przypadku Google Drive, który jest oznaczony kolorowym trójkątem. W ramach serwerów Google następuje proces deszyfracji plików, co obrazują grafiki opatrzone literami A-E. Następnie dane powracają do użytkownika. Transmisja z serwera Google do użytkownika (numer 8) jest ponownie zaszyfrowana.[132]

---

[129] *G Suite Encryption Whitepaper*, https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf, str. 3, dostęp na dzień 8 lipca 2020 r.
[130] *G Suite Encryption Whitepaper*, https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf, str. 9, dostęp na dzień 8 lipca 2020 r.
[131] *G Suite Encryption Whitepaper*, https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf, str. 9, dostęp na dzień 8 lipca 2020 r.
[132] *G Suite Encryption Whitepaper*, https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf, str. 6, dostęp na dzień 8 lipca 2020 r.



[źródło grafiki: „G Suite Encryption Whitepaper", https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf, str. 7, dostęp na dzień 8 lipca 2020 r.]

21. [pozostałe kwestie]

142. W przypadku tej chmury dostawca zapewnia również inne, dodatkowe narzędzia związane z bezpieczeństwem przechowywanych danych. Administratorzy danych mogą przykładowo określić, że niektóre pliki (np. zawierające szczególnie istotne informacje) nie będą mogły być pobierane, drukowane, kopiowane czy zmieniane przez zwykłych użytkowników.[133]

143. Użytkownicy mają również możliwość korzystania z dwuetapowej weryfikacji (np. przez SMS).[134]

[133] Zob. więcej *G Suite Data Protection Implementation Guide*, grudzień 2018 r., https://cloud.google.com/files/gsuitedataprotectionimplementationguide_012019.pdf, dostęp na dzień 8 lipca 2020 r.
[134] Zob. więcej: *Weryfikacja dwuetapowa*, https://support.google.com/a/answer/175197?hl=pl, dostęp na dzień 8 lipca 2020 r.

144. Administrator ma możliwość przywrócenia plików usuniętych z Dysku Google w ciągu 25 dni od daty ich usunięcia. Może to stanowić zabezpieczenie w sytuacji gdy dojdzie do przypadkowego usunięcia plików, których kopie nie zostały wykonane.

145. Google gwarantuje, że pakiet G Suite (w tym Google Drive) będzie dostępny dla klienta przez 99,9% czasu w danym miesiącu kalendarzowym.[135] Gwarancja w sprawie SLA jest zatem na wysokim poziomie.

VII. ONEDRIVE

22. [informacje wstępne]

146. Aplikacje do pracy biurowej dostarczane przez Microsoft są od lat jednym z podstawowych narzędzi pracy dla radców prawnych. W ramach płatnej platformy Microsoft 365 (dawniej Office 365) można korzystać m.in. z chmury pod nazwą OneDrive. Usługa ta jest dostępna również poza platformą Microsoft 365 – bez konieczności kupowania aplikacji pakietu Office.

147. Dostawcą usługi dla klientów z Polski jest Microsoft Ireland Operations Ltd z siedzibą w Dublinie (Irlandia), choć jak zauważono w Księdze Bezpieczeństwa Komunikacji Elektronicznej w Pracy Radcy Prawnego, podmiot świadczący usługi nie został wprost wskazany w warunkach.[136] Podmiot taki jest określony m.in. na fakturach wystawianych przez Microsoft w związku z korzystaniem z pakietu Microsoft 365. Umowa dotycząca usług Microsoft jest zawierana w oparciu o prawo irlandzkie.

148. Chmura Microsoft działa zarówno na systemach operacyjnych Windows jak i macOS. Z OneDrive'a – podobnie jak z Dysku Google – można korzystać na urządzeniach mobilnych z systemem Android lub iOS.

149. Dostępna jest darmowa wersja tej usługi (z limitem do 5 GB), jednak Microsoft wprost wskazuje, że jest to wersja przeznaczona dla „użytkowników domowych". Dla użytkowników biznesowych Microsoft przewiduje płatne plany taryfowe. W przypadku gdy klient subskrybuje wyłącznie usługę chmury (bez aplikacji pakietu Office), to taka subskrypcja jest odpowiednio tańsza.

---

[135] Gwarancja jakości usług G Suite, https://gsuite.google.com/terms/sla.html, dostęp na dzień 8 lipca 2020 r.
[136] M. Wielisiej, *Analiza porównawcza ogólnej zgodności chmurowych systemów pocztowych: Microsoft Exchange, Google GSuite* [w:] *Księga Bezpieczeństwa Komunikacji Elektronicznej w Pracy Radcy Prawnego*, Krajowa Izba Radców Prawnych, 2020, str. 104.

23. [OneDrive a RODO]

150. Microsoft, podobnie jak Google, deklaruje pełną zgodność swojego działania z przepisami dotyczącymi ochrony danych osobowy (w tym RODO).[137]

151. W ostatnich dniach Europejski Inspektor Ochrony Danych [„EDPS"] wydał rekomendację dla organów i instytucji Unii Europejskiej. Choć trzeba pamiętać, że dotyczą one instytucji UE, to warto się z nimi zapoznać, żeby wiedzieć jakie wątpliwości zgłosił EDPS. Zauważył on, m.in., że problematyczny może być brak kontroli nad tym z jakich subprocesorów korzysta Microsoft oraz braki związane z prawem do przeprowadzenia audytu. Wątpliwości EDPS wzbudziła też m.in. kwestia braku możliwości kontroli lokalizacji danych przetwarzanych przez Microsoft.[138]

152. Jeśli chodzi o przechowywanie danych, to centra danych Microsoft. znajdują się w Azji, Ameryce Południowej, Ameryce Północnej, Australii, Afryce oraz Europie. Microsoft wprost wskazuje, że w przypadku użytkowników z Polski dane zamieszczone przez nich w biznesowej wersji OneDrive są przechowywane w Unii Europejskiej[139]:

Poland

▼ Click to expand

Service	Location
Exchange Online	European Union
OneDrive for Business	European Union

153. Zobowiązanie Microsoft do przechowywania danych w UE w stosunku do użytkowników z tego obszaru wynika również z „Postanowień Dotyczących Usług Online", w których wskazano, że:[140]

Miejsce przechowywania Danych magazynowanych Klienta w przypadku Podstawowych Usług Online
W przypadku Podstawowych Usług Online Microsoft zobowiązuje się przechowywać Dane magazynowane Klienta w określonych głównych obszarach geograficznych (z których każdy zwany jest dalej Obszarem), jak następuje:

- **Usługi Office 365.** Jeśli Klient przydziela zasoby swoim dzierżawcom w Australii, Kanadzie, Unii Europejskiej, Francji, Niemczech, Indiach, Japonii, RPA, Korei Południowej, Szwajcarii, Zjednoczonym Królestwie, Zjednoczonych Emiratach Arabskich lub Stanach Zjednoczonych, Microsoft będzie przechowywać następujące Dane magazynowane Klienta tylko w ramach takiego Obszaru: (1) zawartość skrzynki pocztowej Exchange Online (treść wiadomości e-mail, wpisy w kalendarzu i zawartość załączników wiadomości e-mail), (2) zawartość witryny SharePoint Online i przechowywane w tej witrynie pliki oraz (3) pliki przekazywane do usługi OneDrive dla Firm.

---

[137] Zob. np. https://www.microsoft.com/pl-pl/trust-center/privacy/gdpr-overview, dostęp na dzień 8 lipca 2020 r.

[138] *Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services*, https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_paper_euis_microsoft_contract_investigation_en.pdf, dostęp na dzień 2020 r.

[139] *Where your Microsoft 365 customer data is stored*, https://docs.microsoft.com/en-us/office365/enterprise/o365-data-locations, dostęp na dzień 8 lipca 2020 r.

[140] *Postanowienia Dotyczące Usług Online*, wersja: lipiec 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46, str. 33.

154. OneDrive został zdefiniowany jako jedna z Usług Office 365, a więc to postanowienie ma zastosowanie również do tej usługi.

155. Użytkownicy pakietu Microsoft 365 w ustawieniach swojej organizacji mogą sprawdzić czy znajduje się tam potwierdzenie, że ich dane są przechowywane na terenie UE.

156. Microsoft posiada kilka centrów danych w Unii Europejskiej. Są to następujące lokalizacje: Wiedeń (Austria), Helsinki (Finlandia), Paryż i Marsylia (Francja), Dublin (Irlandia), Amsterdam (Holandia).[141]

157. Microsoft w maju tego roku ogłosił partnerstwo z Operatorem Chmury Krajowej. W ramach tej współpracy Microsoft uruchomi w Polsce pierwszy region przetwarzania danych w Europie Środkowo-Wschodniej. [142] Część danych będzie wówczas przetwarzana na terenie naszego kraju.

158. Microsoft udostępnia dokument pod nazwą „Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft" [„Dodatek"], który zawiera szczegółowe informacje na temat zasad przetwarzania danych osobowych w ramach swoich usług.[143] Dokument ten jest cyklicznie aktualizowany, a ostatnia polska wersja pochodzi z lipca 2020 r. (metadane wskazują na datę 1 lipca 2020 r.). W ostatnich dniach Microsoft udostępnił wersję angielską zaktualizowaną na dzień 21 lipca 2020 r.[144]

159. W najnowszej angielskiej wersji odnotowano wydanie przez TSUE wyroku ws. C-311/18 i m.in. wskazano, że Tarcza Prywatności nie stanowi dłużej podstawy do transferu danych do USA.[145] Microsoft utrzymuje jednak, że podstawą transferu danych osobowych poza Europejski Obszar Gospodarczy są standardowe klauzule umowne. Nie wskazano jednak, by postanowienie to było wyłączone w stosunku do USA, a zatem należy uznać, że Microsoft utrzymuje, iż klauzule dalej mogą być podstawą przekazania danych do USA. Potwierdza zamieszczony od razu po wyroku komunikat na stronie internetowej Microsoft[146]:

---

[141] *Where your Microsoft 365 customer data is stored*, https://docs.microsoft.com/en-us/office365/enterprise/o365-data-locations, dostęp na dzień 8 lipca 2020 r.
[142] https://chmurakrajowa.pl/cloud-journal/2020-05-05-post/, dostęp na dzień 8 lipca 2020 r.
[143] *Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft*, wersja: Lipiec 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=dpa
[144] *Microsoft Online Services Data Protection Addendum*, wersja: 21 lipca 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=dpa
[145] *Microsoft Online Services Data Protection Addendum*, wersja: 21 lipca 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=dpa, str. 10
[146] *Assuring Customers About Cross-Border Data Flows*, https://blogs.microsoft.com/eupolicy/2020/07/16/assuring-customers-about-cross-border-data-flows/, 16 lipca 2020 r., dostęp na dzień 25 lipca 2020 r.

We want to be clear: if you are a commercial or public sector customer, you can continue to use Microsoft services in compliance with European law. The Court's ruling does not change your ability to transfer data today between the EU and U.S. using the Microsoft cloud.

For years we have provided customers with overlapping protections under both the Standard Contractual Clauses (SCCs) and Privacy Shield frameworks for data transfers. Although today's ruling invalidated the use of Privacy Shield moving forward, the SCCs remain valid. Our customers are already protected under SCCs.

160. Jak wskazano wyżej, w przypadku biznesowych użytkowników z Polski, ich dane przechowywane w ramach usługi OneDrive są domyślnie przetwarzane na terenie Unii Europejskiej. Pozornie nie powinno być zatem problemu związanego z transferem danych do USA. Jak jednak wskazano w Księdze Bezpieczeństwa Komunikacji Elektronicznej w Pracy Radcy Prawnego: „Microsoft […] rozpoznał swoją rolę jako administratora danych o użytkownikach i danych technicznych/telemetrycznych. 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."[147]

161. Microsoft wprost wskazuje w Dodatku, że dane telemetryczne (określane w Dodatku jako dane diagnostyczne) mogą zawierać dane osobowe.[148] Przy takim założeniu kwestia dopuszczalności transferu danych telemetrycznych do USA na podstawie standardowych klauzul nabiera zatem bardzo istotnego znaczenia. Jeśli bowiem przeważy wykładania, zgodnie z którą do USA nie można przekazywać nawet danych telemetrycznych, to ta praktyka będzie musiała zostać zmieniona.

162. Co do zasady Microsoft w stosunku do danych klienta przechowywanych na OneDrive'ie pełni rolę podmiotu przetwarzającego w rozumieniu art. 28 RODO.

163. Dodatek określa wyraźnie przedmiot przetwarzania, czas trwania przetwarzania, charakter i cel przetwarzania, kategorie przetwarzanych danych, a więc elementy określone w art. 28 ust. 3 RODO.

164. W Dodatku potwierdzono, że dostawca przetwarza dane osobowe wyłącznie na udokumentowane polecenie klienta. Umowa licencjonowania zbiorowego zawarta przez klienta (na której treść składa się również Dodatek), dokumentacja produktu oraz sposób używania i konfigurowania przez klienta usług stanowią – w świetle treści Dodatku - ostateczne udokumentowane instrukcje klienta dla

[147] M. Gawroński, M. Ćwiakowski, P. Szurmak, *Ocena zgodności wykorzystywania usług wideokonferencyjnych Teams, Zoom, Webex w działalności radców prawnych*, [w:] *Księga Bezpieczeństwa Komunikacji Elektronicznej w Pracy Radcy Prawnego*, Krajowa Izba Radców Prawnych, 2020, str. 23; na temat roli Microsoft jako niezależnego administratora zob. również *Microsoft Online Services Data Protection Addendum*, wersja: 21 lipca 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=dpa, str. 7.

[148] *Microsoft Online Services Data Protection Addendum*, wersja: 21 lipca 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=dpa, str. 5.

Microsoft w zakresie przetwarzania danych osobowych.[149] Umowa zawierana z Microsoft spełnia więc warunek wskazany w art. 28 ust. 3 lit. a RODO.

165. Microsoft zapewnia, że jego personel (a więc osoby mające dostęp do danych osobowych klienta) jest zobowiązany do zachowania poufności i zabezpieczenia wszelkich danych, nawet po zakończeniu okresu zatrudnienia.[150] Umowa spełnia więc warunek wskazany w art. 28 ust. 3 lit. b RODO.

166. W Dodatku znajduje się deklaracja, że Microsoft „wdroży oraz będzie utrzymywać odpowiednie zabezpieczenia o charakterze technicznym i organizacyjnym" w celu ochrony danych klienta.[151] Zabezpieczenia stosowane przez Microsoft są opisane w Aneksie A do Dodatku oraz innych materiałach, a zatem użytkownik powinien oprócz zapoznania się z Dodatkiem odnaleźć i zapoznać się z dodatkowymi dokumentami. W naszej ocenie przy takim opisie zabezpieczeń można uznać, że spełniony jest warunek z art. 28 ust. 3 lit. c RODO.

167. Standardem w przypadku takich podmiotów jak Microsoft jest korzystanie z usług subprocesorów. Nie inaczej jest w tym przypadku. Klient akceptując Dodatek wyraża zgodę na korzystanie przez Microsoft z podmiotów podprzetwarzających dane.[152] Microsoft zapewnia, że nakłada na te podmioty obowiązki związane z ochroną danych co najmniej na takim samym poziomie na jakim są obowiązki nałożone na Microsoft na podstawie Dodatku. Z Dodatku wynika jedynie, że informacja o subprocesorach znajduje się „w witrynie Microsoft". Faktycznie taka lista jest dostępna na stronie servicetrust.microsoft.com.[153] W trakcie trwania umowy z klientem Microsoft może zaangażować nowe podmioty podprzetwarzające. W takim przypadku dostawca powiadomi klienta o tym fakcie. Klient, który nie zaakceptuje nowego subprocesora może wypowiedzieć swoją subskrypcję. W naszej ocenie takie postanowienia powodują, że za spełniony można uznać warunek określony w art. 28 ust. 3 lit. d w zw. z art. 28 ust. 2 i 4 RODO.

168. Zgodnie z Dodatkiem, Microsoft udostępni klientom możliwość realizacji wniosków osób, których dotyczą dane, o wykonanie ich praw wynikających z RODO[154], co jest zgodne z warunkiem określonym w art. 28 ust. 3 lit. e RODO. W portalu administracyjnym usługi Microsoft udostępnia pulpit nawigacyjny

---

[149] *Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft*, wersja: Lipiec 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=dpa, str. 8.
[150] *Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft*, wersja: Lipiec 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=dpa, str. 11.
[151] *Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft*, wersja: Lipiec 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=dpa, str. 9.
[152] *Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft*, wersja: Lipiec 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=dpa, str. 11-12.
[153] *Microsoft Online Services Subprocessors List*, 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.
[154] *Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft*, wersja: Lipiec 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=dpa, str. 8.

ułatwiający zarządzaniem sprawami związanymi ze zgłoszeniami osób których dane dotyczą, co może być przydatnym narzędziem w organizacjach, które otrzymują dużo takich zgłoszeń.

169. W Dodatku znajduje się również ogólna deklaracja, że Microsoft pomaga Klientowi wywiązać się z obowiązków określonych w art. 32–36 RODO[155], co jest wymagane przez art. 28 ust. 3 lit. f RODO.

170. Microsoft usuwa dane klienta po upływie 90 dni od wygaśnięcia lub wypowiedzenia przez klienta subskrypcji.[156]

171. Microsoft udostępnia klientom wyniki audytów dotyczących zabezpieczeń komputerów, środowiska informatycznego i fizycznych centrów przetwarzania danych używanych przez Microsoft. Z Dodatku zdaje się wynikać, że klient może zgłosić Microsoft, że chciałby przeprowadzić dodatkowy audyt (nie polegający tylko na weryfikacji dokumentacji). Microsoft deklaruje, że jest to możliwe i udostępni „systemy przetwarzania, placówki i dokumentację pomocniczą związaną z przetwarzaniem Danych Klientów i Danych Osobowych przez Microsoft, podmioty stowarzyszone Microsoft i Podmioty Podprzetwarzające Microsoft." [157] Audyt powinien być jednak przeprowadzony przez niezależny podmiot. W razie stwierdzenia nieprawidłowości Microsoft zobowiązuje się do ich usunięcia. Choć można mieć pewne wątpliwości, to w naszej ocenie takie zobowiązanie jest zgodne z art. 28 ust. 3 lit. h RODO.

172. Microsoft zobowiązuje się do powiadamiania bez zbędnej zwłoki klienta o stwierdzonym naruszeniu zabezpieczeń prowadzącym do zniszczenia, utraty, zmiany, nieupoważnionego ujawnienia lub uzyskania dostępu do danych klienta. Dostawca zbada każdy taki przypadek i podejmie kroki w celu ograniczenia jego skutków.[158]

173. Microsoft podkreśla, że posiada certyfikaty m.in. takie jak: ISO/IEC 27001 (Zarządzanie Bezpieczeństwem Informacji), ISO/IEC 27017 (Bezpieczeństwo w Chmurze), ISO/IEC 27018 (Ochrona Danych Osobowych w Chmurze)[159].

174. Podobnie jak w przypadku Google, w naszej ocenie, biorąc pod uwagę treść umowy powierzenia przetwarzania danych oraz treść dokumentów publikowanych przez Microsoft, nie ma powodów by twierdzić, że korzystanie z OneDrive jest niezgodne z RODO, chociaż w tym przypadku również

---

[155] *Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft,* wersja: Lipiec 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=dpa, str. 28.
[156] *Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft*, wersja: Lipiec 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=dpa, str. 11.
[157] *Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft*, wersja: Lipiec 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=dpa, str. 10.
[158] *Dodatek dotyczący Ochrony Danych w ramach Usług Online Microsoft*, wersja: Lipiec 2020 r., https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=2&Keyword=dpa, str. 10.
[159] https://servicetrust.microsoft.com/ViewPage/MSComplianceGuideV3, dostęp na dzień 8 lipca 2020 r.

trzeba bardzo ostrożnie podchodzić do kwestii danych przekazywanych poza EOG w kontekście wyroku ws. Schrems II.

24. [szyfrowanie w OneDrive]

175. Na stronach internetowych związanych z usługą Microsoft 365 znaleźć można liczne informacje, w których Microsoft opisuje szyfrowanie stosowane w dostarczanych usługach. Część z tych informacji pochodzi sprzed zmiany nazwy z Office 365 na Microsoft 365, jednak zakładamy, że używane zabezpieczenia się nie zmieniły, a informacje skoro nadal są dostępne, pozostają aktualne.

176. Microsoft informuje, że dane użytkowników są szyfrowane zarówno „w spoczynku" jak i „w trakcie przesyłu". Dostawca wprost wskazuje, że szyfrowanie obejmuje również pliki, które są przesyłane i przechowywane w OneDrive.[160] Nie odnaleźliśmy informacji, aby jakiś rodzaj plików był wyłączony z szyfrowania, tak jak ma to miejsce w przypadku plików wideo i Dysku Google.

177. Dostawca deklaruje, że w przypadku usługi OneDrive zastosowanie znajduje polityka „zero-standing access", która oznacza, że pracownicy Microsoft nie mają dostępu do usługi, chyba że dostęp zostanie im udzielony w wyniku konkretnego incydentu.[161] W tym przypadku również nie mamy więc do czynienia z modelem „zero-knowledge encryption". Microsoft ma potencjalną możliwość wglądu w dane klienta, który musi zaakceptować deklaracje dostawcy, że ten stosuje restrykcyjne środki bezpieczeństwa ograniczające ryzyko nieautoryzowanego dostępu do tych danych.

178. Jeżeli chodzi o ochronę danych „w spoczynku", to można również odnaleźć informacje, że Microsoft stosuje:

1) środki ochrony fizycznej, które polegają na tym, że do centrów danych ma dostęp ograniczona liczba osób, których tożsamość jest weryfikowana;

2) ochronę sieci, która polega na stosowaniu firewall'i ograniczających ruch z nieautoryzowanych lokalizacji;

3) zabezpieczenia aplikacji, które polegają m.in. na automatycznych i ręcznych analizach w celu identyfikacji możliwych usterek;

4) ochronę zawartości (content'u), która polega na szyfrowaniu plików w stanie spoczynku unikatowym kluczem AES256.[162]

---

[160] *Encryption*, https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption?view=o365-worldwide, dostęp na dzień 8 lipca 2020 r.
[161] *How OneDrive safeguards your data in the cloud*, https://support.microsoft.com/en-us/office/how-onedrive-safeguards-your-data-in-the-cloud-23c6ea94-3608-48d7-8bf0-80e142edd1e1, dostęp na dzień 8 lipca 2020 r.
[162] *How OneDrive safeguards your data in the cloud*, https://support.microsoft.com/en-us/office/how-onedrive-safeguards-your-data-in-the-cloud-23c6ea94-3608-48d7-8bf0-80e142edd1e1, dostęp na dzień 8 lipca 2020 r.

179. W centrach danych tego dostawcy jest wykorzystywany jest BitLocker, czyli rozwiązanie pozwalające na szyfrowanie przy pomocy algorytmu AES (128-bitowego lub 256-bitowego). BitLocker jest używany na poziomie szyfrowania dysków. Rozwiązanie to może być zresztą wykorzystywane również na komputerach użytkowników, którzy korzystają z systemu Windows.[163] BitLocker jest używany także do szyfrowania „w spoczynku" tych danych, które zostały przesłane do OneDrive'a.[164]

180. Oprócz BitLocker'a, który szyfruje dyski, Microsoft stosuje szyfrowanie na poziomie plików. W tym celu używa unikalnych kluczy szyfrowania dla poszczególnych plików („per-file encryption"). W przypadku tego szyfrowania dostawca stosuje 256-bitowy klucz AES.[165] Pliki wgrane do OneDrive są dzielone na „kawałki", a następnie każdy „kawałek" jest szyfrowany 256-bitowym kluczem AES.[166]

181. Korzystając z usług tego dostawcy klient może również liczyć na szyfrowanie „w trakcie przesyłu". Szyfrowanie danych „w trakcie przesyłu" może nastąpić gdy:

1) urządzenie użytkownika (np. komputer) komunikuje się z serwerami Microsoft;

2) serwer Microsoft komunikuje się z innym serwerem Microsoft.

182. W przypadku wersji OneDrive dla firm szyfrowanie na etapie użytkownik – serwer Microsoft następuje z użyciem protokołów SSL/TLS i 2048-bitowych kluczy.[167]

183. Szyfrowanie transmisji pomiędzy serwerami Microsoft również następuje w oparciu o protokół TLS lub o zbiór protokołów IPsec.[168] Microsoft deklaruje, że nie zezwala na połączenia przez protokół HTTP i przekierowuje użytkowników do szyfrowanej wersji protokołu HTTP, czyli HTTPS.[169]

184. Microsoft wykorzystuje i wspiera TLS w wersji 1.2. W informacji datowanej na 15 czerwca 2020 r. Microsoft wskazuje, że pakiet Office 365 nie wspiera TLS w wersji 1.3.[170]

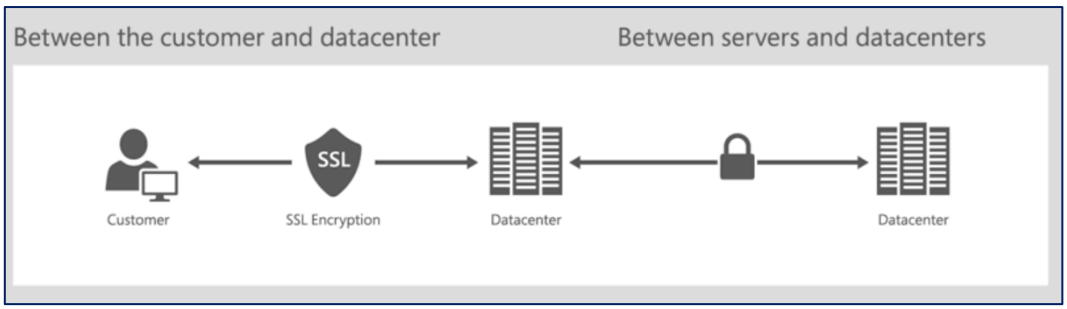
---

[163] Zob. więcej https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview, dostęp na dzień 8 lipca 2020 r.
[164] *Data Encryption in OneDrive for Business and SharePoint Online*, https://docs.microsoft.com/en-us/microsoft-365/compliance/data-encryption-in-odb-and-spo?view=o365-worldwide, dostęp na dzień 8 lipca 2020 r.
[165] *Data Encryption in OneDrive for Business and SharePoint Online*, https://docs.microsoft.com/en-us/microsoft-365/compliance/data-encryption-in-odb-and-spo?view=o365-worldwide, dostęp na dzień 8 lipca 2020 r.
[166] *Encryption for Skype for Business, OneDrive for Business, SharePoint Online, Microsoft Teams, and Exchange Online*, https://docs.microsoft.com/pl-pl/microsoft-365/compliance/office-365-encryption-for-skype-onedrive-sharepoint-and-exchange?view=o365-worldwide, dostęp na dzień 8 lipca 2020 r.

I. **[167] *Data Encryption in OneDrive for Business and SharePoint Online*, https://docs.microsoft.com/en-us/microsoft-365/compliance/data-encryption-in-odb-and-spo?view=o365-worldwide, dostęp na dzień 8 lipca 2020 r.**

[168] *Encryption for data in transit*, https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-for-data-in-transit?view=o365-worldwide, dostęp na dzień 8 lipca 2020 r.
[169] *How OneDrive safeguards your data in the cloud*, https://support.microsoft.com/en-us/office/how-onedrive-safeguards-your-data-in-the-cloud-23c6ea94-3608-48d7-8bf0-80e142edd1e1, dostęp na dzień 8 lipca 2020 r.
[170] *Technical reference details about encryption*, https://docs.microsoft.com/en-us/microsoft-365/compliance/technical-reference-details-about-encryption?view=o365-worldwide, dostęp na dzień 8 lipca 2020 r.

185. Szyfrowanie „w trakcie przesyłu” Microsoft podsumowuje graficznie w następujący sposób:



[źródło: fragment filmu dostępnego pod następującym linkiem: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-encryption-in-odb-and-spo?view=o365-worldwide]

25. [pozostałe kwestie]

186. Użytkownicy OneDrive’a mają do dyspozycji również dodatkowe narzędzia umożliwiające zabezpieczenie plików. Jednym z nich jest Customer Key. To narzędzie pozwala zaszyfrować dane użytkownika przechowywane w centrach danych dostawcy kluczami użytkownika. Jest to ciekawe rozwiązanie pozwalające zapewnić dodatkową ochronę, jednak korzystanie z niego wymaga znajomości specyfiki szyfrowania i usług Microsoft.

187. Podobnie jak w Google Drive, w przypadku usługi Microsoft, użytkownik może przywrócić usunięte z chmury dane (np. jeśli zrobił to przypadkowo). Ma na to 30 dni.

188. Microsoft gwarantuje, że OneDrive będzie dostępny dla klienta przez 99,9% czasu.[171] Gwarancja w sprawie SLA jest zatem na wysokim poziomie, podobnie jak w przypadku Google Drive.

VIII. iCLOUD DRIVE

26. [informacje wstępne]

189. Chmurą, z której wiele osób korzysta prywatnie na co dzień jest iCloud Drive dostarczana przez Apple. Jest to usługa będąca częścią pakietu iCloud, przeznaczona dla użytkowników sprzętu Apple (komputerów Mac, iPhone’ów czy iPad’ów). Osoby używające innych urządzeń mogą korzystać z tej chmury przez przeglądarkę internetową lub np. aplikację iCloud dla Windows.

190. W przypadku użytkowników z Unii Europejskiej spółką odpowiedzialną za dostarczenie usługi jest Apple Distribution International Ltd. z siedzibą w Hollyhill Industrial Estate, Hollyhill, Cork (Republika Irlandii).

[171] *Umowa dotycząca Poziomu Usług Online Microsoft*, wersja: 1 lipiec 2020 r. https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37.

191. Pliki przechowywane w tej chmurze są dostępne na wszystkich urządzeniach Apple, z których korzysta dany użytkownik. Użytkownik iCloud Drive może udostępnić foldery i dokumenty innym osobom. Zaproszone osoby mogą pobierać udostępniany folder lub plik na swoje urządzenia. iCloud Drive służy jednak co do zasady do zapewnienia jednemu użytkownikowi dostępu do plików na różnych jego urządzeniach (w oparciu o logowanie o to samo Apple ID). Nie jest to więc chmura, której całą zawartość w standardowej jej wersji można byłoby udostępnić wszystkim członkom danej organizacji.

192. Dodatkowo trzeba koniecznie zwrócić uwagę na jedno z postanowień warunków korzystania z usług Apple, zgodnie z którym „Użytkownik dodatkowo przyjmuje do wiadomości i akceptuje, że Usługa została zaprojektowana i jest przeznaczona do użytku prywatnego przez jedną osobę, i że nie powinien ujawniać innym osobom informacji o Koncie i/lub hasła."[172] Takie postanowienie regulaminu naszym zdaniem powoduje, że standardowo pakiet iCloud jest dedykowany konsumentom i nie powinien być używany komercyjnie.

193. Taką tezę zdaje się potwierdzać okoliczność, że w przypadku standardowej usługi iCloud, Apple nie umożliwia użytkownikom zawarcia umowy powierzenia przetwarzania danych. Te okoliczności powodują, że naszym zdaniem należy ostrożnie podejść do korzystania ze standardowej wersji iCloud w działalności zawodowej radców prawnych (dotyczy to nie tylko iCloud Drive, ale wszystkich elementów przetwarzanych w ramach usług iCloud, a mogą to być np. kontakty, wiadomości, notatki – jeżeli treści te są przesyłane do chmury Apple).

194. Takie stanowisko dotyczy – jak już wspomniano – standardowej wersji usług Apple, z których może korzystać bezpłatnie każdy użytkownik sprzętu tego przedsiębiorstwa. Apple komunikuje bowiem na swoich stronach internetowych, że posiada rozwiązania, które pozwalają korzystać z ich rozwiązań w biznesie.[173]

195. Wśród wielu informacji dotyczących komercyjnego użycia produktów i usług Apple znajdują się takie, z których wynika, że usługa iCloud Drive może być wykorzystywana nie tylko do „użytku prywatnego"[174]:

[172] Pkt IV. A warunków, https://www.apple.com/legal/internet-services/icloud/pl/terms.html, dostęp na dzień 8 lipca 2020 r.
[173] Zob. np. https://www.apple.com/pl/business/, dostęp na dzień 8 lipca 2020 r.
[174] https://www.apple.com/pl/business/it/, dostęp na dzień 8 lipca 2020 r.

Zarządzane konta Apple ID dla pracowników.

Firma sama tworzy konta i zarządza nimi. Są one jej własnością i działają zarówno na prywatnych urządzeniach pracowników, jak i urządzeniach firmowych. Dzięki usłudze Apple Business Manager zarządzane konta Apple ID można tworzyć dla pracowników automatycznie. Służą im one do zespołowej pracy z wykorzystaniem aplikacji i usług Apple, a także dają dostęp do danych związanych z pracą w aplikacjach zarządzanych korzystających z iCloud Drive. A jeśli organizacja korzysta z rejestracji użytkownika, pracownicy mogą używać na własnych urządzeniach nie tylko zarządzanego, ale też prywatnego konta Apple ID.

196. Apple Business Manager to portal internetowy, który ułatwia wdrażanie sprzętów Apple w przedsiębiorstwie.[175] W naszej ocenie należałoby jednak zadać dodatkowe pytania Apple związane z korzystaniem z tej usługi, ponieważ jej opis oraz konsekwencje korzystania z niej nie są dla nas jasno i precyzyjnie wskazane.

197. Zgodnie z umową dotyczącą usługi Apple Business Manager [„Umowa ABM"], jeśli użytkownik jest z Unii Europejskiej, to umowa podlega prawu i sądom w Irlandii.

27. [iCloud Drive a RODO]

198. W Umowie ABM znajdują się postanowienia dotyczące danych osobowych, które zostały przez nas przeanalizowane.[176] Sposób redakcji postanowień nie jest w pełni przejrzysty z uwagi na to, że postanowienia zostały zamieszczone w kilku zaledwie jednostkach redakcyjnych i są zapisane w sposób ciągły – to znaczy w jednej jednostce redakcyjnej znajdują się postanowienia dotyczące różnych kwestii.

199. Zgodnie z Umową ABM, Apple działa jako podmiot przetwarzający dane w imieniu użytkownika. Zawierając tę umowę użytkownik upoważnia Apple do przetwarzania i używania danych osobowych w celu świadczenia usługi (pkt 9.1 Umowy ABM). Zawarcie Umowy ABM będzie więc trzeba traktować również jako zawarcie umowy powierzenia przetwarzania z Apple. W przeciwieństwie do Google i Microsoft, postanowienia dotyczące danych nie zostały więc wprowadzone w osobnym dokumencie. Choć może wpływać to nieco na przejrzystość kontraktu, to nie jest niedopuszczalne.

200. Zgodnie z Umową ABM „zaszyfrowane Dane osobowe mogą być przechowywane w lokalizacji znanej tylko Apple" (pkt 9.3 Umowy ABM). Apple wydaje się traktować oświadczenie dosłownie. Oczywiście

---

[175] Zob. więcej *Podręcznik użytkownika usługi Apple Business Manager*, https://support.apple.com/pl-pl/guide/apple-business-manager/apdd344cdd9d/web, dostęp na dzień 8 lipca 2020 r.
[176] Umowa jest dostępna pod następującym linkiem: https://business.apple.com/#enrollment, dostęp na dzień 8 lipca 2020 r.

dostawca informuje o tym gdzie znajdują się jego centra danych, ale nie udało nam się odnaleźć informacji, która potwierdzałaby, że użytkownik ma możliwość wyboru by dane były przechowywane np. na terenie Unii Europejskiej. Może to wynikać również z tego, że (o czym będzie jeszcze mowa), do przechowywania danych użytkowników iCloud wykorzystywane są serwery należące do Amazon i Google. Apple korzysta tu więc z rozwiązań zewnętrznych.

201. W przypadku Apple należy więc założyć, że dochodzi do transferu danych poza EOG. Jak wskazuje dostawca w pkt. 9.4 Umowy ABM:

> Jeżeli będzie to wymagane przez prawo, Apple zapewni, że dane przekazywane w ramach międzynarodowych transferów będą przesyłane wyłącznie do krajów, które zapewniają odpowiedni poziom ochrony, wprowadziły odpowiednie zabezpieczenia określone w obowiązujących przepisach prawa, takich jak art. 46. i 47. RODO (np. standardowe klauzule ochrony danych) lub podlegają odstępstwu na mocy art. 49. RODO. Jeśli Użytkownik jest zobowiązany do zawarcia umowy o przekazywaniu danych w celu przekazania ich do kraju trzeciego, wyraża on zgodę na zawarcie w ramach swojej jurysdykcji odpowiedniej umowy o przekazywaniu danych zgodnie z informacjami udostępnionymi przez Apple na stronie https://apple.com/legal/enterprise/datatransfer.

202. Dokonując transferu danych Apple korzysta ze standardowych klauzul umownych.[177]

203. W naszej ocenie warto spróbować nawiązać z Apple kontakt w celu ustalenia czy istnieje możliwość wyboru opcji przetwarzania danych wyłącznie na terytorium Unii Europejskiej. Mając na uwadze potencjalne skutki uzasadnienia wyroku TSUE ws. Schrems II trzeba pamiętać, że przekazywanie danych do USA na podstawie standardowych klauzul może być ryzykowne. Ewentualnie należy spróbować ustalić, czy przy korzystaniu z usług Apple możliwe jest stosowanie dodatkowych zabezpieczeń. Rozważyć można też stosowanie innej podstawy prawnej przekazania danych, ale o to w przypadku działalności takiej jak prowadzą radcy prawni może w praktyce być trudno.

204. Podobnie jak w przypadku Google i Microsoft, przeanalizowaliśmy postanowienia dotyczące powierzenia przetwarzania danych Apple.

205. Apple zwraca uwagę na to, że przetwarzanie odbywa się m.in. zgodnie z instrukcjami udzielonymi przez użytkownika udzielonymi za pośrednictwem usługi lub pisemnie (pkt 9.1 Umowy ABM), co można uznać za spełnienie warunku, o którym mowa w art. 28 ust. 3 lit. a RODO.

206. Z analizowanego dokumentu wynika, że dostawca „podejmie odpowiednie kroki w celu zapewnienia przestrzegania procedur bezpieczeństwa przez jego pracowników i wykonawców" oraz „dołoży wszelkich starań, by wszelkie osoby upoważnione do przetwarzania takich Danych osobowych przestrzegały obowiązujących przepisów dotyczących poufności i bezpieczeństwa" (pkt 9.3 Umowy

[177] Apple opublikował standardowe klauzule pod tym linkiem: https://www.apple.com/legal/enterprise/data-transfer-agreements/datatransfer-pl.pdf, dostęp na dzień 8 lipca 2020 r.

ABM). W tym zakresie można więc ostatecznie uznać, że umowa spełnia warunek wskazany w art. 28 ust. 3 lit. b RODO.

207. Apple informuje o tym, że stosuje standardowe środki do ochrony danych osobowych podczas ich przesyłania, przetwarzania i przechowywania. Dostawca stosuje „ekonomicznie uzasadnione wysiłki w celu szyfrowania danych", „zapewnienia nieprzerwanej poufności, spójności, dostępności i odporności", a także „przywrócenia dostępności Danych osobowych w odpowiednim czasie w przypadku problemów" oraz „regularnego sprawdzania, oceniania i ewaluacji takich środków" (pkt 9.3 Umowy ABM). Są to deklaracje, które powinny oczywiście znaleźć się w umowie (stosownie do art. 28 ust. 3 lit c RODO), jednak w przypadku Google i Microsoft w umowach powierzenia przetwarzania danych znajdował się opis konkretnych środków technicznych i organizacyjnych podejmowanych przez tych dostawców. W przypadku Umowy ABM taki opis nie został zamieszczony. Apple wskazuje jedynie, że pomaga użytkownikowi w zapewnieniu zgodności z art. 32 RODO przez „wdrożenie procedur bezpieczeństwa określonych w niniejszym rozdziale 9.3. oraz utrzymanie certyfikatów ISO 27001 i ISO 27018".

208. Apple podobnie jak Google i Microsoft wskazuje, że zawarcie umowy jest jednoznaczne z udzieleniem Apple zgody na korzystanie z usług subprocesorów pod warunkiem, że podmioty takie są umownie zobowiązane do zapewnienia co najmniej takiej samej ochrony jak tak, do której zobowiązało się Apple (pkt 9.1 Umowy ABM). Nie udało nam się jednak odnaleźć listy takich podmiotów. Nie udało nam się odnaleźć również informacji na temat możliwości wyrażenia sprzeciwu co do korzystania przez Apple z usług danego subprocesora ani na temat tego w jaki sposób Apple informuje o tym, że zamierza skorzystać z usług nowego subprocesora. Obowiązek takiego informowania i możliwości wyrażenia sprzeciwu przez administratora wynika z art. 28 ust. 2 RODO i art. 28 ust. 3 lit. d RODO. W przypadku iCloud Drive Apple informuje (w innym materiale), że korzysta z usług Google i Amazon. Mogą to więc być subprocesorzy Apple.[178]

209. Apple w sposób lakoniczny informuje również o procedurze odpowiadania na wnioski osób, które zgłosiły żądania dotyczące ich danych osobowych (pkt 9.1 Umowy ABM). Apple przesądza, że to użytkownik jest odpowiedzialny za odpowiedź na wniosek, co jest oczywiście naturalne, jednak brak postanowień dotyczących tego jak dostawca wspiera użytkownika w wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III RODO, o czym stanowi art. 28 ust. 3 lit. e RODO.

210. Apple deklaruje, że będzie pomagać użytkownikom w zapewnieniu zgodności z art. 33 i 34 RODO (a więc w sprawach zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu oraz zawiadamiania osób, których dane dotyczą, o naruszeniu ochrony ich danych) oraz art. 35 i 36 RODO

[178] *Omówienie kwestii bezpieczeństwa w usłudze iCloud*, https://support.apple.com/pl-pl/HT202303, dostęp na dzień 8 lipca 2020 r.

(a więc przepisami, które obligują użytkownika do przeprowadzenia oceny skutków w zakresie ochrony danych lub konsultacji z organem nadzorczym). Warunek określony w art. 28 ust. 3 lit. f należy uznać za spełniony.

211. Po zakończeniu świadczenia usług Apple „zobowiązuje się do zniszczenia w bezpieczny sposób i w rozsądnym terminie Danych osobowych przechowywanych przez Apple" (pkt 9.4 Umowy ABM). W przeciwieństwie do Google i Microsoft, Apple nie deklaruje wprost terminu usunięcia danych. Pomimo tego można uznać, że warunek z art. 28 ust. 3 lit. g RODO jest spełniony.

212. Apple umożliwia użytkownikom przeprowadzenie audytu jednak „pod warunkiem, że posiadane przez Apple certyfikaty ISO 27001 i ISO 27018 zostaną uznane za wystarczające do przeprowadzenia wymagane audytu" (pkt 9.3 Umowy ABM). Trudno przesądzić sens tego postanowienia, jednak brzmi ono w sposób, który sugeruje, że audyt ma polegać na weryfikacji dokumentacji przedstawionej przez Apple. Gdyby tak było, to można mieć wątpliwości, czy warunek z art. 28 ust. 3 lit. h RODO został spełniony.

213. Apple zobowiązuje się do powiadamiania użytkownika (bez zbędnej zwłoki) o tym, że doszło do zmiany, usunięcia lub utracenia danych w wyniku nieuprawnionego dostępu do usługi (pkt 9.2 Umowy ABM).

214. Podobnie jak pozostali dostawcy, Apple informuje precyzyjnie o tym jakie certyfikaty ISO posiada. I tak, z przedstawionych informacji wynika, że[179]:

> Apple Inc. utrzymuje certyfikaty w zgodności z normami ISO 27001 i 27018, aby umożliwić klientom firmy Apple realizację zobowiązań regulacyjnych i umownych. Certyfikaty te stanowią niezależne poświadczenie praktyk firmy Apple w zakresie bezpieczeństwa informacji i ochrony prywatności dotyczących systemów wchodzących w ich zakres.

215. Apple wprost podaje, że usługi iCloud i Apple Business Manager są objęte obiema wskazanymi normami ISO.[180]

216. W naszej ocenie, w przypadku postanowień Umowy ABM istnieją wątpliwości czy spełniają one wymogi wynikające z RODO. Deklaracje i zobowiązania Apple są słabsze niż deklaracje i zobowiązania Microsoft i Google. Dodatkowo pojawiają się wątpliwości związane z kontrolą nad korzystaniem przez Apple z subprocesorów oraz możliwością zmiany lokalizacji danych. Z pewnością

[179] *Certyfikaty usług internetowych Apple*, https://support.apple.com/pl-pl/HT210897, dostęp na dzień 8 lipca 2020 r.
[180] *Certyfikaty usług internetowych Apple*, https://support.apple.com/pl-pl/HT210897, dostęp na dzień 8 lipca 2020 r.

kwestie zaznaczone powyżej jako budzące wątpliwości, należałoby spróbować wyjaśnić z Apple, a być może uda się uzyskać satysfakcjonujące odpowiedzi.

28. [szyfrowanie w iCloud Drive]

217. Apple deklaruje, że usługa iCloud została opracowana przy użyciu „standardowych w branży technologii" zabezpieczeń i obowiązują w niej rygorystyczne zasady związane z ochroną informacji.[181]

218. W przypadku iCloud Drive, Apple potwierdza, że stosuje zarówno szyfrowanie „w spoczynku" jak i „w trakcie przesyłu". Dostawca wskazuje również, że stosuje bezpieczne tokeny do uwierzytelniania a szyfrowanie odbywa się z użyciem szyfru AES z kluczem 128-bitowym. [182]

219. Apple (podobnie jak Microsoft) nie podaje informacji, z których wynikałoby, że jakiś rodzaj plików (np. wideo) nie jest szyfrowany „w spoczynku". Zakładamy zatem, że szyfrowane są wszystkie pliki.

220. Dostawca deklaruje, że do przechowywania danych osobowych użytkownika „stosuje systemy komputerowe z ograniczonym dostępem znajdujące się w fizycznie zabezpieczonych pomieszczeniach".[183]

221. Każdy plik przechowywany w iCloud (a więc również w usłudze chmury) „dzielony jest na fragmenty i szyfrowany przez iCloud przy użyciu standardu AES-128 oraz klucza generowanego przy użyciu funkcji SHA-256 na podstawie zawartości każdego fragmentu. Klucze i metadane plików są przechowywane przez Apple na koncie iCloud użytkownika."[184]

222. Pliki przechowywane w usłudze iCloud Drive są zgodnie z informacjami przekazanymi przez Apple chronione dodatkowo[185]:

---

[181] *Omówienie kwestii bezpieczeństwa w usłudze iCloud*, https://support.apple.com/pl-pl/HT202303, dostęp na dzień 8 lipca 2020 r.
[182] *Omówienie kwestii bezpieczeństwa w usłudze iCloud*, https://support.apple.com/pl-pl/HT202303, dostęp na dzień 8 lipca 2020 r.
[183] *Zasady ochrony prywatności*, https://www.apple.com/legal/privacy/pl/, dostęp na dzień 8 lipca 2020 r.
[184] *Bezpieczeństwo platform Apple (Wiosna 2020),* https://manuals.info.apple.com/MANUALS/1000/MA1902/pl_PL/apple-platform-security-guide-pl.pdf, str. 86, dostęp na dzień 8 lipca 2020 r.
[185] *Bezpieczeństwo platform Apple (Wiosna 2020),* https://manuals.info.apple.com/MANUALS/1000/MA1902/pl_PL/apple-platform-security-guide-pl.pdf, str. 86, dostęp na dzień 8 lipca 2020 r.

> iCloud Drive chroni dodatkowo dokumenty przechowywane w iCloud przy użyciu kluczy konta. Zawartość plików na iCloud Drive jest dzielona na fragmenty i szyfrowana, a zaszyfrowane fragmenty są przechowywane przy użyciu usług innych firm. Klucze zawartości plików są jednak opakowywane przy użyciu kluczy rekordów przechowywanych razem z metadanymi iCloud Drive. Klucze rekordów są chronione przy użyciu klucza usługi iCloud Drive użytkownika, który jest przechowywany na koncie iCloud użytkownika. Użytkownicy uzyskują dostęp do metadanych swoich dokumentów w iCloud po uwierzytelnieniu na iCloud, ale w celu dostępu do chronionych części w iCloud Drive muszą także mieć klucz usługi iCloud Drive.

223. Tak jak wskazywaliśmy wcześniej, Apple informuje, że w niektórych przypadkach do przechowywania danych mogą być wykorzystywane serwery należące do Amazon lub Google. Apple deklaruje, że dane w formie zaszyfrowanej przechowuje także w przypadku gdy wykorzystywane są zewnętrzne rozwiązania do przechowywania danych.[186] Podkreśla również, że partnerzy tacy jak Amazon czy Google nie mają kluczy umożliwiających odszyfrowanie danych przechowywanych na ich serwerach.[187]

224. W spoczynku są szyfrowane również dane przechowywane w ramach kopii zapasowych (backup'ów). Apple stosuje w tym przypadku co najmniej szyfrowanie AES z kluczem 128-bitowym.[188] Używane jest również uwierzytelnienie za pomocą tokenów bezpieczeństwa.[189]

225. Apple potwierdza także, że dane w iCloud Drive są szyfrowane także podczas transferu (czyli wg naszej terminologii – „w trakcie przesyłu").

226. Systemy operacyjne Apple obsługują protokół TLS (w wersjach 1.0, 1.1, 1.2, 1.3) oraz DTLS[190]. Protokół TLS obsługuje standardy AES-128 oraz AES-256 i preferuje używanie zestawów szyfrów z utajnianiem z wyprzedzeniem.[191]

---

[186] *Zasady ochrony prywatności*, https://www.apple.com/legal/privacy/pl/, dostęp na dzień 8 lipca 2020 r.
[187] *Omówienie kwestii bezpieczeństwa w usłudze iCloud*, https://support.apple.com/pl-pl/HT202303, dostęp na dzień 8 lipca 2020 r. oraz *Bezpieczeństwo platform Apple (Wiosna 2020)*, https://manuals.info.apple.com/MANUALS/1000/MA1902/pl_PL/apple-platform-security-guide-pl.pdf, str. 86, dostęp na dzień 8 lipca 2020 r.
[188] *Omówienie kwestii bezpieczeństwa w usłudze iCloud*, https://support.apple.com/pl-pl/HT202303, dostęp na dzień 8 lipca 2020 r.
[189] *Bezpieczeństwo platform Apple (Wiosna 2020),* https://manuals.info.apple.com/MANUALS/1000/MA1902/pl_PL/apple-platform-security-guide-pl.pdf, str. 86, dostęp na dzień 8 lipca 2020 r.
[190] „TLS może także działać za pośrednictwem protokołu transportu UDP (User Datagram Protocol), który jest używany do transmisji „bezpołączeniowych, jak ruch głosowy lub wideo. Jednak w przeciwieństwie do TCP, UDP nie gwarantuje dostarczenia lub poprawnej kolejności pakietów. TLS w wersji dla UDP jest więc nieco inny i nosi nazwę DTLS (Datagram Transport Layer Security)", Jean-Philippe Aumasson, *Nowoczesna kryptografia,* Wydawnictwo Naukowe PWN, 2018, str. 354.
[191] *Bezpieczeństwo platform Apple (Wiosna 2020),* https://manuals.info.apple.com/MANUALS/1000/MA1902/pl_PL/apple-platform-security-guide-pl.pdf, str. 125, dostęp na dzień 8 lipca 2020 r.

227. Zabezpieczenie „w trakcie przesyłu" oznacza zabezpieczenie połączenia od urządzenia użytkownika do serwerów dostawcy usługi. Apple podkreśla, że szyfrowanie to ma miejsce „na całej drodze przesyłu".[192]

228. Dostawca zabezpiecza tworzone backup'y nie tylko przez ich przechowywanie w formie zaszyfrowanej, ale także szyfrując je podczas przesyłania przez internet.[193]

29. [pozostałe kwestie]

229. Apple informuje o tym, że w ramach ich usług można skorzystać z tzw. „kompleksowego szyfrowania danych". Ten rodzaj szyfrowania oznacza, że dostęp do danych ma jedynie użytkownik. Nawet dostawca usługi 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 dane przechowywane w usłudze iCloud Drive.[194]

IX. REKOMENDACJE

230. Stosowanie chmury jest coraz bardziej popularne w różnych sektorach gospodarki, również tych, w których w sposób szczególny dba się o poufność danych, podobnie jak w przypadku radców prawnych.[195] Biorąc pod uwagę, że chmura już teraz jest standardem w biznesie oraz to, że dobrze sprawdza się również w codziennej pracy w kancelariach prawnych, należy naszym zdaniem wykonać kolejny krok i z pytania o to, czy radcowie prawni mogą korzystać z chmury przejść do pytania o to, jak powinni oni korzystać z chmury w sposób bezpieczny.

231. Założeniem tego opracowania nie było rekomendowanie korzystania z usług konkretnego dostawcy. Chcieliśmy jedynie zwrócić uwagę na konkretne postanowienia regulaminów lub deklaracje usługodawców, których odnalezienie niekiedy nie jest proste. Celem było więc zebranie danych potrzebnych radcom do oceny ryzyka związanego z korzystaniem z rozwiązań chmurowych oraz przekazanie informacji o tym, jakie kwestie radca prawny powinien zweryfikować i jakie dane uzyskać, w przypadku gdyby chciał korzystać z usług innego dostawcy. Na rynku funkcjonuje bowiem oczywiście mnóstwo innych rozwiązań chmurowych, które oferują podobne parametry i warunki do które analizowaliśmy w tym opracowaniu. Każdy z radców prawnych może więc dobrać odpowiednie dla siebie narzędzie.

---

[192] *Bezpieczeństwo platform Apple (Wiosna 2020),* https://manuals.info.apple.com/MANUALS/1000/MA1902/pl_PL/apple-platform-security-guide-pl.pdf, str. 88,
[193] *Bezpieczeństwo platform Apple (Wiosna 2020),* https://manuals.info.apple.com/MANUALS/1000/MA1902/pl_PL/apple-platform-security-guide-pl.pdf, str. 86, dostęp na dzień 8 lipca 2020 r.
[194] *Omówienie kwestii bezpieczeństwa w usłudze iCloud*, https://support.apple.com/pl-pl/HT202303, dostęp na dzień 8 lipca 2020 r.
[195] Zob. np. *Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej*, 23 stycznia 2020 r.

232. W przypadku korzystania z chmur publicznych (takich jak opisane w tym opracowaniu), trzeba się pogodzić, że pozostanie pewna strefa, co do której nie uda się usunąć wszystkich wątpliwości. Sygnalizowaliśmy wyżej problem konieczności zachowania w poufności wszystkich informacji objętych tajemnicą zawodową – również w przypadku korzystania z chmury. Przyjrzyjmy się zatem chociażby kwestii ujawniania tajemnicy radcowskiej. Zgodnie z art. 3 ust. 5 u.r.p. radca prawny nie może być zwolniony z obowiązku zachowania tajemnicy zawodowej co do faktów, o których dowiedział się udzielając pomocy prawnej lub prowadząc sprawę. Z kolei art. 180 § 2 k.p.k. wskazuje w jakich przypadkach radcowie prawni mogą być przesłuchani co do faktów objętych tajemnicą. Radca prawny ma obowiązek podjęcia wszelkich przewidzianym prawem środków dla uniknięcia lub ograniczenia określonego w przepisach prawa zwolnienia go z obowiązku zachowania tajemnicy zawodowej (art. 19 KERP).

233. Tymczasem w wielu regulaminach usług znajdują się ogólne postanowienia, zgodnie z którymi dane klienta mogą być ujawnione przez dostawcę w związku z prowadzonymi postępowaniami sądowymi. Takie postanowienia oczywiście nie uwzględniają kwestii tajemnicy radcowskiej. Trudno się zresztą temu dziwić, ponieważ chmura publiczna jest oparta na standardzie, który nie uwzględnia takich kwestii. Trzeba jednak dodać, że zwykle dostawcy deklarują jednak, że w przypadku ujawnienia danych innemu podmiotowi, poinformują o tym fakcie klienta.

234. Osoby obawiające się potencjalnego naruszenia tajemnicy radcowskiej powinny zatem:

1) korzystać z narzędzi pozwalających na zaszyfrowanie plików bezpośrednio na urządzeniu, a następnie przysłać pliki do chmury już w formie zaszyfrowanej lub

2) używać chmury opartej na szyfrowaniu uniemożliwiających dostawcy wgląd do treści danych, czyli „zero-knowledge encryption”.

235. Podsumowując, uważamy że korzystanie z przechowywania plików w chmurze przez radców prawnych jest dopuszczalne, jednak powinni oni podjąć działania, które zminimalizują ryzyko naruszenia zasad etyki i przepisów o ochronie danych osobowych.

236. Po pierwsze, zupełnie podstawową kwestią powinna być weryfikacja regulaminu usługi i sprawdzenie czy nie ma w nim postanowień wykluczających jej zastosowanie w biznesie lub postanowień, które budzą wątpliwości z punktu widzenia potencjalnej ochrony danych lub tajemnicy zawodowej. Choć decydujące znaczenie ma nie tyle to, czy usługa jest darmowa czy płatna, ale właśnie konkretne postanowienia regulaminu, to trzeba pamiętać, że w przypadku darmowych chmur, ryzyko znalezienia w regulaminie postawień, które nie mogą być zaakceptowane jest większe (na przykład postanowień upoważniających usługodawcę do wykorzystywania przechowywanych przez klienta danych w celach marketingowych).

237. Po drugie, po wstępnym zweryfikowaniu, czy usługa w ogóle nadaje się do biznesowego użycia, należy zwrócić uwagę na kwestię bezpieczeństwa gwarantowanego przez usługodawcę. Pod uwagę można wziąć przykładowo elementy, o których pisaliśmy w tym opracowaniu, czyli przede wszystkim stosowane środki bezpieczeństwa oraz gwarantowany poziom SLA. Wybrany powinien zostać dostawca, którego deklaracje 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. W naszej ocenie radca prawny powinien również pamiętać o tym, by kontrolować tę kwestię także już po wyborze dostawcy. W przypadku gdyby pojawiły się np. informacje o wycieku danych z usługi, z której radca już korzysta, to powinien on podjąć odpowiednie działania i zdecydować o tym, czy będzie z tej usługi korzystał w dalszym ciągu, czy jednak dokona migracji.

238. Po trzecie, należy zweryfikować czy oferowana przez dostawcę umowa powierzenia przetwarzania danych spełnia wymogi RODO.

239. Po czwarte, koniecznie należy ustalić jak wygląda kwestia przekazywania danych poza EOG i czy w świetle wyroku TSUE ws. Schrems II nie występuje zwiększone ryzyko.

240. Po piąte, radca prawny powinien poinformować klienta o potencjalnych zagrożeniach związanych z chmurą. W naszej ocenie dobrą praktyką powinno być umożliwienie klientowi zgłoszenia sprzeciwu co do takiego sposobu przechowywania jego plików. W sytuacji gdy klient nie zgadza się na to by jego dane były przesyłane do chmury, radca prawny powinien zastosować się do takiego oczekiwania klienta.

241. Po szóste, radca prawny powinien wykonywać regularnie kopie zapasowe plików przechowywanych w chmurze. Bardzo istotne jest by nie utracić dostępu do wszystkich plików w przypadku awarii serwerów dostawcy lub np. zablokowania konta klienta. Wykonywanie backupów pozwoli na przynajmniej częściowe „uniezależnienie" się od usługodawcy.

242. Po siódme, w przypadku najbardziej „wrażliwych" informacji rozważyć można przechowywanie ich poza chmurą – np. wyłącznie lokalnie na dysku komputera. Koniecznie trzeba jednak zadbać o wykonanie kopii zapasowych takich danych i zabezpieczeniu nośników, na których te kopie będą przechowywane (np. przez korzystanie z szyfrowanego pendrive'a). Dobrą praktyką może być określenie wewnętrznej polityki, która będzie przesądzać o tym jakie pliki można przechowywane w chmurze a jakie nie. Alternatywą może być stosowanie narzędzi umożliwiających zaszyfrowanie plików lokalnie i przesłanie ich w formie zaszyfrowanej do chmury. Nawet dostawca usługi chmurowej nie będzie wówczas mógł ich odczytać.

Damian Kortowski

Karol Wątrobiński

radca prawy Damian Nartowski

radca prawny Karol Wątrobiński