Komisja
LegalTech
Okręgowej Izby
Radców Prawnych
w Warszawie

MARUTA \

STANDARD PRZETWARZANIA INFORMACJI W CHMURZE OBLICZENIOWEJ

PRZEZ RADCÓW PRAWNYCH

SPIS TREŚCI

I. JAK KORZYSTAĆ ZE STANDARDU? ... 3
II. JAK KORZYSTAĆ Z ZAŁĄCZNIKÓW DO STANDARDU? ... 3
III. SCHEMAT POSTĘPOWANIA W ZWIĄZKU Z ZAMIAREM KORZYSTANIA Z USŁUGI CHMUROWEJ ... 5
IV. ZASADY SZCZEGÓŁOWE ... 6
1. Staranność w doborze Dostawcy ... 6
2. Klasyfikacja i ocena informacji ... 6
3. SZACOWANIE RYZYKA W ZAKRESIE PODSTAWOWYM ... 8
4. Szacowanie ryzyka w pełnym zakresie ... 10
5. Strategia postępowania z ryzykiem ... 12
6. Transparentność ... 13
7. Rozliczalność ... 13
8. Odpowiedzialność Radcy prawnego ... 13
9. Definicje ... 14
10. Załączniki ... 16

I. JAK KORZYSTAĆ ZE STANDARDU?

I.1. Niniejszy standard określa zasady postępowania w przypadku decyzji radcy prawnego o korzystaniu z usług chmury obliczeniowej. Standard powinien być stosowany:

I.1.1. niezależnie od rodzaju informacji, które Radca prawny zamierza przetwarzać w chmurze obliczeniowej w związku z wykonywaniem czynności zawodowych, niezależnie od formy wykonywania zawodu;

I.1.2. w odniesieniu do korzystania z chmury publicznej lub hybrydowej. W przypadku korzystania z usług chmury prywatnej rekomenduje się, by Radca prawny brał pod uwagę Standard w niezbędnym zakresie.

I.2. Przed rozpoczęciem korzystania z usług chmury obliczeniowej Radca prawny powinien:

I.2.1. dokonać oceny dostawcy pod kątem rękojmi, jaką daje w zakresie bezpieczeństwa i jakości świadczonej usługi (**Rozdział IV.2**);

I.2.2. przeprowadzić klasyfikację informacji oraz dokonać oceny informacji pod kątem dopuszczalności jej przetwarzania w chmurze obliczeniowej (**Rozdział IV.3**);

I.2.3. oszacować ryzyko, związane z przetwarzaniem informacji w chmurze obliczeniowej w zakresie podstawowym (**Rozdział IV.4**) lub pogłębionym (**Rozdział IV.5**)

I.2.4. określić zasady postępowania z ryzykiem (**Rozdział IV.6**);

I.2.5. poinformować klientów o korzystaniu z chmury obliczeniowej, np. poprzez stosowną informację na stronie internetowej (**Rozdział IV.7**);

I.2.6. zapewnić rozliczalność wszystkich podejmowanych działań (**Rozdział IV.8);**

I.3. Uproszczony schemat kluczowych czynności w ramach tego procesu zawarty jest poniżej.

I.4. Standard obowiązuje niezależnie od formy wykonywania zawodu – praktyczna realizacja poszczególnych założeń może jednak różnić się w zależności od tego w jakiej formie Radca prawny wykonuje zawód oraz jaką funkcję pełni w jednostce organizacyjnej. Szczegóły w tym zakresie opisane są w **Rozdziale IV.9.**

I.5. Definicje stosowane w Standardzie określone są w **Rozdziale IV.10**.

II. JAK KORZYSTAĆ Z ZAŁĄCZNIKÓW DO STANDARDU?

II.1. Do Standardu załączone został szereg dokumentów – narzędzi wspierających Radcę prawnego w zachowaniu zgodności. Do załączników tych należy:

II.1.1. Załącznik nr 1 – Checklista zgodności

Radca prawny może oprzeć się na checkliście by zweryfikować, czy proces przygotowania się do rozpoczęcia korzystania z usług chmury obliczeniowej został przeprowadzony zgodnie ze Standardem.

II.1.2. Załącznik nr 2 – Rekomendacje dla radców prawnych

Rekomendacje stanowią rozwinięcie zasad opisanych w niniejszym Standardzie. Zawierają analizę poszczególnych wytycznych. Radca prawny może opierać się na nich w razie konieczności dokonania pogłębionej wykładni zasad zawartych w Standardzie.

II.1.3. Załącznik nr 3 – Wzór procedury klasyfikacji i oceny informacji

Wzór może stanowić podstawę lub inspirację dla Radcy prawnego do wdrożenia rozwiązań organizacyjnych w zakresie klasyfikacji i oceny informacji w jego organizacji. Do wzoru załączone jest narzędzie wspierające proces klasyfikacji i oceny informacji. Skorzystanie z niego zapewni, że wszystkie elementy określone standardem zostanie uwzględnione przez Radcę prawnego.

Wzory dokumentów, przed ich wdrożeniem przez Radcę prawnego, powinny zostać dostosowane do uwarunkowań jego praktyki. Przykłady

II.1.4. Załącznik nr 4 – Wzór procedury szacowania ryzyka

Wzór może stanowić podstawę lub inspirację dla Radcy prawnego do wdrożenia rozwiązań organizacyjnych w zakresie szacowania ryzyka w związku z korzystaniem z usług chmury obliczeniowej.

Do wzoru załączone jest narzędzie wspierające proces szacowania ryzyka. Skorzystanie z niego zapewni, że wszystkie elementy określone standardem zostanie uwzględnione przez Radcę.

Szacowanie ryzyka odnosi się do ryzyk związanych inherentnie z chmurą obliczeniową i nie zastępuje oceny ryzyka prowadzonej na podstawie przepisów odrębnych, w szczególności w zakresie ochrony danych osobowych, W tym zakresie pomocne mogą być inne opracowania, takie jak np. Księga Bezpieczeństwa Komunikacji Elektronicznej w pracy Radcy Prawnego (wydana przez Krajową Izbę Radców Prawnych).

II.1.5. Załącznik nr 5 i 6 – Przykład szacowania ryzyka dla usługi Google Docs w ramach G Suite oraz dla usługi Microsoft Office 365

Załącznik zawiera przykładowo wypełnione narzędzie służące szacowaniu ryzyka. Celem jest zaprezentowanie Radcy prawnemu sposobu posługiwania się narzędziem w praktyce oraz ułatwienie mu formułowania wniosków z analizy w popularnych usługach chmurowych.

Radca prawny, posiłkując się przykładem powinien jednak zapewnić, że prowadzona przez niego szacowanie ryzyka uwzględnia konkretne uwarunkowania jego działalności (nie należy stosować metody „kopiuj–wklej”).

III. SCHEMAT POSTĘPOWANIA W ZWIĄZKU Z ZAMIAREM KORZYSTANIA Z USŁUGI CHMUROWEJ

INWENTARYZACJA

CEL: Ustalenie stanu faktycznego, identyfikacja celu procesu i zasobów informacyjnych wykorzystywanych w procesie
OSOBA ODPOWIEDZIALNA: Koordynator, wyznaczony Radca prawny lub prawnik działający pod nadzorem Radcy Prawnego

- Ustalenie **PRZEBIEGU PROCESU**
- **ZGROMADZENIE INFORMACJI** nt. aktualnie stosowanych zasad klasyfikacji informacji i szacowania ryzyka
- **ZGROMADZENIE DOKUMENTÓW** wymagających analizy (umowy z dostawcą, regulaminy, procedury wewnętrzne)

KLASYFIKACJA I OCENA INFORMACJI

CEL: Ustalenie stanu faktycznego, identyfikacja celu procesu i zasobów informacyjnych wykorzystywanych w procesie
OSOBA ODPOWIEDZIALNA: Koordynator, wyznaczony Radca prawny lub prawnik działający pod nadzorem Radcy Prawnego

- **PRZYPISANIE ZASOBÓW** informacyjnych wykorzystywanych w procesie do klas
- **OCENA WYSTĘPOWANIA PRZESŁANEK** ograniczających lub wyłączających
- **OCENA WAŻNOŚCI INFORMACJI** i jej charakteru
- Oszacowanie **SKALI PROCESU**

WSTĘPNA DECYZJA O SKORZYSTANIU Z CHMURY

OSOBA ODPOWIEDZIALNA: Zarządzający

SZACOWANIE RYZYKA

CEL: Identyfikacja ryzyk i zarządzenie nimi
OSOBA ODPOWIEDZIALNA: Koordynator, wyznaczony Radca prawny lub prawnik działający pod nadzorem Radcy Prawnego, ze wsparciem osoby posiadającej kompetencje techniczne

- **IDENTYFIKACJA ZAGROŻEŃ** związanych z korzystaniem z chmury obliczeniowej
- **OKREŚLENIE WPŁYWU** materializacji zagrożenia **i prawdopodobieństwa** jego wystąpienia
- Oszacowanie ryzyka początkowego i określenie **ŚRODKÓW ZARADCZYCH**
- Określenie ryzyka szczątkowego i **STRATEGII POSTĘPOWANIA Z RYZYKIEM**

DECYZJA O SPOSOBIE POSTĘPOWANIA Z RYZYKIEM

OSOBA ODPOWIEDZIALNA: Zarządzający

WDROŻENIE I STOSOWANIE ŚRODKÓW ZARADCZYCH

CEL: Minimalizacja zidentyfikowanych ryzyk, rozliczalność procesu
OSOBA ODPOWIEDZIALNA: Koordynator, wyznaczony Radca prawny lub prawnik działający pod nadzorem Radcy Prawnego

- **WYZNACZENIE OSÓB ODPOWIEDZIALNYCH** za zarządzanie ryzykami
- Prowadzenie **BIEŻĄCEGO MONITOROWANIA** ryzyk
- **DOKUMENTOWANIE** podejmowanych działań

ROZPOCZĘCIE KORZYSTANIA Z USŁUGI

MONITOROWANIE RYZYKA

OSOBA ODPOWIEDZIALNA: Koordynator, wyznaczony Radca prawny lub prawnik działający pod nadzorem Radcy Prawnego

IV. ZASADY SZCZEGÓŁOWE

1. ZGODNOŚĆ Z PRAWEM

1.1. Radca prawny w każdym wypadku korzystania z chmury obliczeniowej powinien zapewnić zgodność usługi z przepisami prawa oraz zasadami etyki zawodowej. Wszystkie wymogi zawarte w Standardzie powinny być interpretowane w świetle tej zasady ogólnej.

2. STARANNOŚĆ W DOBORZE DOSTAWCY

2.1. Radca prawny powinien zapewnić, że korzysta z usług Dostawcy Usług chmury obliczeniowej dającego rękojmie należytego świadczenia usług w zakresie:

2.1.1. zgodności z prawem i zasadami deontologii radcowskiej;

2.1.2. adekwatnego poziomu bezpieczeństwa informacji;

2.1.3. adekwatnego poziomu dostępności Usługi chmurowej w kontekście ciągłości gotowości do świadczenia pomocy prawnej.

2.2. Radca prawny powinien być w stanie wykazać przeprowadzenie oceny Dostawcy w zakresie spełnienia warunków, o których mowa w pkt 2.1

3. KLASYFIKACJA I OCENA INFORMACJI

3.1. Przed rozpoczęciem korzystania z chmury obliczeniowej, Radca prawny powinien zapewnić dokonywanie klasyfikacji i oceny informacji przy uwzględnieniu, że:

3.1.1. klasyfikacja informacji powinna odnosić się co najmniej do tych wszystkich informacji, które są lub mają być przetwarzane w chmurze obliczeniowej;

3.1.2. klasyfikacja informacji powinna opierać się na jasno określonym kryterium, w szczególności takim kryterium może być waga skutków naruszenia bezpieczeństwa informacji dla Radcy prawnego;

3.2. Przykładowo klasyfikacja informacji może opierać się na następującym podziale:

3.2.1. Klasa A – informacje publiczne

Klasa obejmuje informacje, które mogą być ujawniane osobom trzecim (na zewnątrz Kancelarii) bez żadnych ograniczeń, a ich utrata nie ma negatywnych skutków dla Kancelarii.

3.2.2. Klasa B – informacje wewnętrzne

Klasa obejmuje informacje, które mogą być ujawniane personelowi Kancelarii oraz w miarę potrzeby także podwykonawcom / Dostawcom.

3.2.3. Klasa C – informacje ważne

Klasa obejmuje informacje, niepodlegające zaliczeniu do klasy D lub E, które z uwagi na swą wagę lub powiązane z nimi wymaganie prawne powinny być ujawniane jedynie uprawnionym osobom lub podmiotom (wewnątrz Kancelarii lub osobom trzecim), z zachowaniem szczególnych warunków.

3.2.4. Klasa D – informacje szczególnie chronione

Klasa obejmuje informacje objęte tajemnicą radcowską, stanowiące treść pomocy prawnej, o ile nie podlegają one zaklasyfikowaniu do klasy E.

3.2.5. Klasa E – informacje zastrzeżone

Klasa obejmuje informacje, które z uwagi na swą wagę lub powiązane z nimi wymaganie prawne z zasady nie powinny być ujawniane osobom lub podmiotom innym, niż te, które wytworzyły informacje, najwyższemu kierownictwu i podmiotom przez nie wskazanym.

3.3. Radca prawny powinien zapewnić dokonywanie oceny informacji w celu ustalenia czy i na jakich zasadach dopuszczalne jest przetwarzanie informacji w chmurze obliczeniowej. Ocena informacji powinna uwzględniać w szczególności:

3.3.1. zakładaną lub faktyczną skalę przetwarzania informacji w chmurze obliczeniowej;

3.3.2. charakter przetwarzanej informacji;

3.3.3. ważność informacji;

3.3.4. występowanie ograniczeń kontraktowych lub organizacyjnych wpływających na dopuszczalność korzystania z chmury obliczeniowej.

3.4. Ocena występowania ograniczeń kontraktowych lub organizacyjnych wpływających niedopuszczalność korzystania z chmury obliczeniowej powinna uwzględniać w szczególności zobowiązania względem klientów lub osób trzecich, wewnętrzne regulacje i standardy a także obowiązek transparentnej i budzącej zaufanie komunikacji względem Klientów lub osób trzecich.

3.5. Ocena informacji powinna być oparta o jasno zdefiniowane kryteria.

3.6. Klasyfikacja i ocena informacji powinna odbywać się cyklicznie, nie rzadziej niż raz na rok oraz za każdym razem:

3.6.1. dla każdej planowanej do wykorzystania lub wykorzystywanej Usługi chmury obliczeniowej;

3.6.2. dla każdego nowego rodzaju informacji który Radca prawny zamierza przetwarzać w procesie;

3.6.3. po wystąpieniu następujących zdarzeń: zmiana prawa, regulacji, regulaminów lub postanowień umów, które to zmiany mogą wpływa wpływać na zgodność postępowania Radcy prawnego w kontekście przetwarzania informacji w chmurze obliczeniowej;

3.6.4. zwiększenia lub zmniejszania skali przetwarzania informacji w procesie;

3.6.5. w przypadku istotnego zwiększenia się ważności przetwarzanych informacji.

3.7. Klasyfikacja i ocena informacji powinna odbywać się w oparciu o udokumentowany proces. Wyniki przeprowadzonej klasyfikacji i oceny informacji powinny zostać utrwalone w postaci pisemnej lub elektronicznej, w sposób zapewniający identyfikację osoby dokonującej czynności oraz integralność sporządzonej informacji.

4. SZACOWANIE RYZYKA W ZAKRESIE PODSTAWOWYM

4.1. W przypadku, gdy przetwarzanie w chmurze nie będzie obejmować informacji stanowiących tajemnicę zawodową ani nie będzie dotyczyć informacji o wysokim poziomie ważności, Radca prawny może ograniczyć analizę ryzyka do:

4.1.1. stwierdzenia zgodności z prawem, w szczególności zgodności z prawem ochrony danych osobowych umowy z Dostawcą Usługi chmury obliczeniowej;

W tym zakresie Radca prawny powinien co najmniej:

- w zakresie informacji objętej tajemnicą zawodową, zapewnić, że Dostawca zobowiązał się do zachowania informacji w tajemnicy w formie dokumentowej;
- w zakresie informacji objętej tajemnicą zawodową, zapewnić, że Dostawca zobowiązał się do posługiwania się osobami zobowiązanymi do tajemnicy w formie dokumentowej;
- zapewnić, że Dostawca zobowiązał się do niewykorzystywania informacji objętej tajemnicą zawodową dla własnych celów;
- zapewnić, że informacje stanowiące treść pomocy prawnej, nie są przetwarzane poza Europejskim Obszarem Gospodarczym;
- zapewnić zgodność umowy z wymogami art. 28 RODO;
- zweryfikować prawidłowość i skuteczność mechanizmów dotyczących transferu danych poza EOG (o ile dotyczy);
- przeprowadzić analizę ryzyka dla praw i wolności osób fizycznych (a w razie konieczności – DPIA);
- zapewnić, że Dostawca informuje o podwykonawcach, wraz z zakresem świadczonych usług oraz informuje Radcę prawnego o zmianach na liście;
- zapewnić, że umowa z Dostawcą nie narusza przepisów prawa ani standardów etyki zawodowej.

4.1.2. stwierdzenia adekwatności zabezpieczeń technicznych i organizacyjnych oferowanych przez Dostawcę Usługi chmury obliczeniowej;

W tym zakresie Radca prawny powinien co najmniej:

- zapewnić szyfrowanie informacji objętych tajemnicą zawodową zawsze at rest i in transit
- zapewnić stosowanie nieskompromitowanych algorytmów szyfrowania
- zapewnić, że Dostawca wdrożył system kontroli dostępu do informacji
- zapewnić, że Dostawca stosuje zasadę domyślnego braku dostępu do przetwarzanych informacji (secure-by-default)
- uzyskać od Dostawcy, w przypadku przetwarzania informacji, stanowiących tajemnicę zawodową, deklarację zgodności ze standardami: SOC2 Type 2, Tier III wg Uptime Institute, klasa 3 wg PN-EN 50600;
- zapewnić, że Dostawca zobowiązuje się do posługiwania się personelem posiadającym odpowiednie kompetencje techniczne i do jego regularnego szkolenia
- zapewnić, że informacje stanowiące treść pomocy prawnej, nie są przechowywane poza Europejskim Obszarem Gospodarczym (również w sytuacjach awaryjnych)
- w odniesieniu do informacji stanowiących treść pomocy prawnej, korzystanie z usług wsparcia wyłącznie w oparciu o zindywidualizowane polecenie klienta usługi
- korzystać, w odniesieniu do informacji stanowiących treść pomocy prawnej, z usług wsparcia świadczonych spoza Europejskiego Obszaru Gospodarczego wyłącznie w oparciu o zindywidualizowane polecenie klienta usługi i po uprzedniej weryfikacji gwarancji poufności ujawnianych informacji;

4.1.3. stwierdzenia adekwatności zabezpieczeń technicznych i organizacyjnych stosowanych przez Radcę prawnego, w związku z korzystaniem z chmury obliczeniowej.

W tym zakresie Radca prawny powinien co najmniej:

- zapewnić regularne szkolenia osób odpowiedzialnych za zarządzanie usługami chmurowymi
- zapewniać szkolenia on – boardingowe i okresowe personelu w zakresie rozpoznawania i zgłaszania incydentów
- wyznaczyć osobę odpowiedzialną za zarządzanie incydentami
- zapewnić, że dostępy uprzywilejowane oraz administracyjne (root) do usług odbywają się z zachowaniem zasad wskazanych w pkt 5.2.5
- określić wewnętrzne zasady w zakresie uruchamiania usług chmurowych, uwierzytelnienia oraz wyznaczyć koordynatora usług chmurowych

4.2. Radca prawny powinien zapewnić, że szacowanie ryzyka odbywa się w udokumentowanym procesie przed rozpoczęciem przetwarzania danych w chmurze oraz w każdym przypadku w razie wystąpienia okoliczności, o których mowa w pkt 3.6.

5. SZACOWANIE RYZYKA W PEŁNYM ZAKRESIE

5.1. W przypadkach innych, niż wskazane w pkt 4.1 Radca prawny zobowiązany jest szacować ryzyko związane z przetwarzaniem informacji w chmurze, szczegółowo dokumentując i opisując zidentyfikowane zagrożenia, oceniając ich wpływ na bezpieczeństwo tajemnicy zawodowej, ciągłość świadczenia pomocy prawnej, finanse i reputację Radcy prawnego oraz szacując prawdopodobieństwo faktycznego wystąpienia zagrożenia.

5.2. Radca prawny szacuje ryzyko, w szczególności z uwzględnieniem, że w odniesieniu do poniższych obszarów ryzyka:

5.2.1. Zgodność z prawem

Radca prawny powinien zapewnić, że korzystanie z Usług chmury obliczeniowej jest zgodne z prawem, w szczególności z zasadami ochrony danych osobowych oraz ochrony tajemnicy zawodowej oraz zasadami deontologii Radcy prawnego.

5.2.2. Ochrona tajemnicy zawodowej

Radca prawny powinien zapewnić, że informacja objęta tajemnicą zawodową nie jest ujawniana osobom, które nie współpracują z Radcą prawnym przy wykonywaniu czynności zawodowych.

Radca prawny powinien zapewnić, że informacja objęta tajemnicą zawodową nie jest wykorzystywana przez osoby trzecie dla własnych celów.

Radca prawny powinien zapewnić, by osoby uzyskujące dostęp do tajemnicy zawodowej zobowiązały się do zachowania informacji w poufności, również po zakończeniu świadczenia usług na rzecz Radcy prawnego.

Przez ujawnienie nie należy rozumieć sytuacji, w której osoba, która nie współpracuje z Radcą prawnym przy wykonywaniu czynności zawodowych uzyskuje dostęp do informacji zaszyfrowanej.

5.2.3. Kompetencje techniczne i zdolności organizacyjne

Radca prawny powinien zapewnić, że osoby uczestniczące w przetwarzaniu informacji w chmurze obliczeniowej, zarówno działające w jego imieniu jak i w imieniu Dostawcy Usługi chmury obliczeniowej, posiadają odpowiednie udokumentowane kompetencje techniczne i zdolności organizacyjne pozwalające na bezpieczne korzystanie z usługi przez Radcę prawnego, w tym w zakresie dokonania niezbędnych konfiguracji i zarządzania usługami.

5.2.4. Bezpieczeństwo organizacyjne i techniczne

Radca prawny powinien zapewnić, że warunki organizacyjne i techniczne przetwarzania informacji odpowiadają wymaganiom zapewnienia bezpieczeństwa

przetwarzania zarówno po stronie dostawcy usług chmury obliczeniowej jak i po stronie radcy prawnego.

W przypadku przetwarzania w chmurze obliczeniowej informacji stanowiących tajemnicę zawodową, Radca prawny powinien wymagać od dostawcy deklaracji zgodności ze standardami: SOC2 Type 2 lub Tier III wg klasyfikacji Uptime Institute, lub klasa 3 wg PN-EN 50600 lub zawarcia w umowie opisu stosowanych zabezpieczeń infrastrukturalnych na równoważnym poziomie.

5.2.5. Kontrola dostępu

Radca prawny powinien zapewnić, że dostęp do informacji przetwarzanych w chmurze obliczeniowej jest nadzorowany.

Radca prawny powinien upewnić się, że dostępy uprzywilejowane oraz administracyjne (*root*) do usług odbywają się z zachowaniem szczególnych zasad bezpieczeństwa:

— realizowane są przez osoby posiadające stosowne upoważnienia radcy prawnego z wykorzystaniem silnego uwierzytelniania (MFA);

— odbywają się z urządzeń oraz sieci zabezpieczonych i regularnie weryfikowanych pod kątem możliwych podatności i nieuprawnionego dostępu.

5.2.6. Szyfrowanie informacji

Radca prawny powinien zapewnić, że informacje objęte tajemnicą zawodową (radcowską lub obrończą) przetwarzane w Usługach chmury obliczeniowej są szyfrowane zawsze „at rest" oraz „in transit", a algorytmy szyfrowania nie są uznane za skompromitowane.

O ile to możliwe i uzasadnione, Radca prawny powinien zapewnić, że w miarę możliwości szyfrowane są także pozostałe informacje przetwarzane przez niego w Usłudze chmury obliczeniowej

5.2.7. Zarządzanie konfiguracjami Usługi chmury obliczeniowej

Radca prawny powinien zapewnić, że stosowane konfiguracje Usług chmurowych są:

— zgodne z wytycznymi Dostawcy Usług chmury obliczeniowej, szczególnie w zakresie konfiguracji bezpieczeństwa przetwarzania;

— adekwatne do sposobu korzystania z Usługi chmurowej i przetwarzanych w ramach Usługi chmurowej informacji.

Radca prawny powinien zapewnić, że wykorzystywane Usługi chmurowe są zarządzane.

5.2.8. Lokalizacja przetwarzania

Radca prawny powinien zapewnić, w przypadku przetwarzania informacji stanowiących treść pomocy prawnej, że dane przetwarzane są na obszarze Unii Europejskiej, również w sytuacjach awaryjnych. Korzystanie z usług wsparcia

świadczonych z lokalizacji poza Unią Europejską w odniesieniu do informacji stanowiących treść pomocy prawnej, jest dopuszczalne tylko przy zachowaniu adekwatnych zabezpieczeń, a dostęp osób trzecich do danych produkcyjnych możliwy jest wyłącznie w przypadku, gdy nie jest technicznie możliwe udzielenie wsparcia bez uzyskiwania takiego dostępu.

5.2.9. Umowa z dostawcą chmury obliczeniowej

Szacowanie ryzyka dotyczącego Umowy z dostawcą chmury obliczeniowej powinno uwzględniać, że:

- w sytuacji, gdy przetwarzane informacje obejmują treść udzielonej pomocy prawnej, umowa powinna być poddana prawu państwa Unii Europejskiej oraz jurysdykcji sądu w państwie Unii Europejskiej;
- umowa powinna jasno odnosić się do właścicielstwa danych i wyłączać możliwość przetwarzania danych objętych tajemnicą zawodową dla własnych celów dostawcy;
- umowa powinna określać obowiązki Dostawcy w zakresie szyfrowania danych, w zakresie wskazanym w pkt 5.2.6
- umowa powinna określać okres przetwarzania danych oraz obowiązek Dostawcy w zakresie usunięcia lub zniszczenia danych po zakończeniu świadczenia Usług chmurowych;
- umowa powinna określać zasady odpowiedzialności Dostawcy za skutki naruszenia bezpieczeństwa przetwarzanych informacji;
- umowa powinna określać poziom zapewnienia dostępności Usługi chmurowej;
- umowa powinna zapewniać mechanizmy w zakresie dostępu do danych w sytuacji zakończenia współpracy z Dostawcą Usług chmurowych w stopniu umożliwiającym zapewnienie ciągłości świadczenia pomocy prawnej.
- umowa powinna określać obowiązek Dostawcy niezwłocznego informowania Radcy prawnego o Incydencie bezpieczeństwa informacji i o naruszeniu ochrony danych osobowych;
- umowa powinna mieć formę pisemną, elektroniczną lub dokumentową.

5.3. Radca prawny powinien zapewnić, że szacowanie ryzyka odbywa się w udokumentowanym procesie przed rozpoczęciem przetwarzania danych w chmurze oraz w każdym przypadku w razie wystąpienia okoliczności, o których mowa w pkt 3.6.

6. STRATEGIA POSTĘPOWANIA Z RYZYKIEM

6.1. Radca prawny podejmuje decyzję o strategii postępowania z ryzykiem uwzględniając wyniki szacowania ryzyka.

6.2. Radca prawny nie powinien akceptować wysokiego ryzyka naruszenia bezpieczeństwa informacji stanowiących treść udzielonej pomocy prawnej.

6.3. Radca prawny powinien monitorować na bieżąco wszystkie zidentyfikowane ryzyka.

6.4. Radca prawny wdraża i stosuje środki zaradcze lub, w zależności od przypadku, zapewnia ich wdrożenie przez osoby, za które ponosi odpowiedzialność lub przez Dostawcę.

7. TRANSPARENTNOŚĆ

7.1. Radca prawny powinien poinformować klientów, co najmniej za pośrednictwem swojej strony internetowej, o fakcie korzystania z Usług chmury obliczeniowej w celu przetwarzania informacji dotyczących klientów, w szczególności informacji objętych tajemnicą zawodową.

8. ROZLICZALNOŚĆ

8.1. Wszystkie działania podejmowane w związku z realizacją niniejszych Wytycznych powinny być realizowane w sposób zapewniający rozliczalność i dokumentowane tak by zapewnić identyfikację osoby dokonującej czynności oraz integralność sporządzonego dokumentu.

9. ODPOWIEDZIALNOŚĆ RADCY PRAWNEGO

9.1. Radca prawny:

9.1.1. wykonujący indywidualną praktykę;

9.1.2. będący wspólnikiem w spółce jawnej lub komandytowej, partnerem lub członkiem Zarządu spółki partnerskiej, uprawnieni do prowadzenia spraw Spółki,

– ponosi odpowiedzialność za stosowanie w Standardu w jednostkach organizacyjnych i zespołach, które mu podlegają.

9.2. W przypadku Radców prawnych kierujących daną specjalizacją w spółce prawniczej lub Kancelarii, można nadać uprawnienia oraz przypisać odpowiedzialność związaną z korzystaniem Usług przetwarzania w chmurze w związku ze świadczoną pomocą prawną. Kierującemu specjalizacją można więc przypisać uprawnienia jak i obowiązki z zakresie nadzoru nad korzystaniem z Usług przetwarzania w chmurze także w stosunku do osób współpracujących z Kancelarią lub spółką (np. specjaliści, eksperci, praktykanci).

STOSUNEK PRACY

9.3. Radca prawny świadczący pracę na podstawie stosunku pracy zatrudniony w przedsiębiorstwie lub w organach administracji państwowej może mieć w praktyce ograniczoną możliwość wpływania na decyzję w zakresie korzystania z chmury obliczeniowej i na przeprowadzenie analizy ryzyka. Radca prawny jest jednak zobowiązany w każdym wypadku:

9.3.1. poinformować przełożonego o konieczności uwzględnienia ochrony informacji objętych tajemnicą zawodową w związku z zakładanym korzystaniem z chmury obliczeniowej;

9.3.2. wskazać na zasadność przeprowadzenia klasyfikacji i oceny informacji oraz szacowania ryzyka w zakresie w jakim zakładane jest korzystanie z chmury obliczeniowej.

9.4. Radcy prawnemu pełniącemu funkcję koordynatora Radców prawnych w rozumieniu Regulaminu wykonywania zawodu może zostać powierzone zadanie koordynowaniem procesu uruchamiania i wykorzystywania narzędzi chmurowych w zakresie związanym z wykonywaniem czynności zawodowych, w tym klasyfikacji i oceny informacji, szacowania ryzyka czy weryfikacji poprawności przypisanych narzędzi kontroli dostępu do Usług chmurowych przez Radców prawnych, standardów bezpieczeństwa korzystania z haseł i innych urządzeń uprawnionych do dostępu do usług. Koordynatorowi może zostać powierzona odpowiedzialność i uprawnienia w powyższy zakresie także wobec innych osób współpracujących z Radcami prawnymi w szczególności jeżeli zostały one zobowiązane do zachowania tajemnicy zawodowej przez Radców prawnych.

APLIKANCI

9.5. Radca prawny powinien kontrolować sposób wykorzystywania Usług przetwarzania w chmurze przez aplikanta. Aplikant natomiast nie może – mając na uwadze zobowiązanie do zachowania tajemnicy zawodowej – samodzielnie korzystać z tych Usług chmurowych bez uzyskania uprzedniej zgody Radcy Prawnego. Patron powinien więc zapoznać aplikanta z zasadami korzystania z usług chmurowych w jednostce organizacyjnej, w której wykonuje zawód i zapewnić odpowiednie przeszkolenia aplikanta.

STAŻYŚCI I PRAKTYKANCI

9.6. Radca prawny powinien zapoznać stażystę lub praktykanta z zasadami korzystania z Usług przetwarzania w chmurze, nadzorować sposób przetwarzania tych informacji w chmurze obliczeniowej i zapewnić, że po zakończeniu praktyki lub stażu osobie go odbywającej odebrany zostanie dostęp do chmury obliczeniowej, w której informację były przetwarzane.

10. DEFINICJE

10.1. **Standard** – niniejszy standard przetwarzania informacji w chmurze, wraz z załącznikami.

10.2. **Radca prawny** – Radca prawny oraz prawnik zagraniczny wpisany na listę prawników zagranicznych.

10.3. **Pracownik** – osoba zatrudniona w Kancelarii w oparciu o umowę o pracę.

10.4. **Współpracownik** – osoba fizyczna współpracująca ze Kancelarią, osobiście wykonująca na jej rzecz zadania w oparciu o umowę cywilnoprawną (np. umowa o współpracy, umowa o dzieło, umowa zlecenia).

10.5. **Kancelaria** – każda organizacyjnoprawna forma wykonywania zawodu radcy prawnego przewidziana w ustawie o radcach prawnych.

10.6. **Zarządzający** – Radca prawny:

10.6.1. wykonujący indywidualną praktykę,

10.6.2. będący wspólnikiem w spółce jawnej lub komandytowej, partnerem lub członkiem Zarządu spółki partnerskiej, uprawnieni do prowadzenia spraw Spółki.

10.7. **Usługi przetwarzania w chmurze, Usługi chmurowe, Usługi w chmurze** – usługa obejmująca udostępnienie współdzielonych dostępnych „na żądanie" przez sieci teleinformatyczne, konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci masowych, aplikacji, usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i minimalnym udziale ich dostawcy.

10.8. **Dostawca usług chmury obliczeniowej** lub **Dostawca** – podmiot, który dysponuje infrastrukturą i oprogramowaniem służącym do świadczenia Usług chmury obliczeniowej oraz świadczy usługi chmury obliczeniowej.

10.9. **Poddostawca** – podmiot, który świadczy usługi dla dostawcy usług chmury obliczeniowej, służące dostarczaniu usługi chmury obliczeniowej i posiada albo może posiadać identyfikowany dostęp do informacji przetwarzanych przez Radcę prawnego.

10.10. **Infrastruktura chmury** – zasoby przetwarzania stanowiące zbiór sprzętu i oprogramowania zapewniające dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych.

10.11. **Incydent bezpieczeństwa** lub **Incydent** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji[1]; incydentem bezpieczeństwa może być w szczególności naruszenie ochrony danych osobowych w rozumieniu RODO.

10.12. **Charakter informacji** – status informacji jako informacji chronionej tajemnicą zawodową (radcowską lub obrończą).

10.13. **Informacje objęte tajemnicą zawodową** lub **Tajemnica zawodowa** – informacje, o których mowa w art. 15 KERP.

10.14. **Kodeks etyki radców prawnych lub KERP** – załącznik do uchwały Nr 3/2014 Nadzwyczajnego Krajowego Zjazdu Radców Prawnych z dnia 22 listopada 2014.

10.15. **Regulamin wykonywania zawodu radcy prawnego lub Regulamin** – załącznik do uchwały Nr 94/IX/2015 Krajowej Rady Radców Prawnych z dnia 13 czerwca 2015 roku.

10.16. **RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) (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).

10.17. **Urp** – ustawa o radach prawnych z dnia 6 lipca 1982 (tj. Dz. U. z 2018 r. poz. 2115).

10.18. **Ustawa AML** – ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (tj. Dz. U. z 2020 r. poz. 971).

[1] Por. norma PN-ISO/IEC 27001:2007

10.19. **Ważność informacji** – właściwość informacji, której wartość określa Radca prawny, uwzględniająca:

10.19.1. status informacji jako objętej tajemnicą radcowską lub obrończą oraz

10.19.2. potencjalny wpływ naruszenia bezpieczeństwa informacji na bezpieczeństwo tajemnicy radcowskiej lub obrończej, ciągłość świadczenia pomocy prawnej, finanse i reputację Radcy prawnego.

10.20. **Skala przetwarzania** – określona przez Radcę prawnego skala przetwarzania, stanowiąca wypadkową kryterium ilościowego (np. liczba rekordów, liczba klientów), oraz kryterium jakościowego (informacje przetwarzane w istotnych / kluczowych procesach lub w procesach subsydiarnych / pomocniczych) w odniesieniu do – odpowiednio – całej działalności Radcy prawnego lub działalności jednostki organizacyjnej, w której wykonuje on zawód.

11. ZAŁĄCZNIKI

11.1. Checklista zgodności

11.2. Rekomendacje dla radcy prawnego

11.3. Wzór procedury klasyfikacji i oceny informacji

11.4. Wzór procedury szacowania ryzyka

11.5. Przykłady szacowania ryzyka dla Google Docs w ramach G Suite oraz Microsoft Office 365