



ADWOKATURA
POLSKA

**DOBRE PRAKTYKI
DOTYCZĄCE
CYBERBEZPIECZEŃSTWA
W DZIAŁALNOŚCI
KANCELARII
ADWOKACKICH
I PRACY ADWOKATA**



Warszawa, 2025

DOBRE PRAKTYKI DOTYCZĄCE CYBERBEZPIECZEŃSTWA W DZIAŁALNOŚCI KANCELARII ADWOKACKICH I PRACY ADWOKATA

Wytyczne i zalecenia dla adwokatów
dotyczące ochrony informacji, zarządzania
ryzykiem oraz budowania odporności cyfrowej
kancelarii, ze szczególnym uwzględnieniem
odpowiedzialnego i bezpiecznego korzystania
z technologii cyfrowych

Wydanie II.
Warszawa 2025



ADWOKATURA
POLSKA



INSTYTUT
LEGALTECH NRA

Wydawca: Naczelna Rada Adwokacka,
ul. Świętojerska 16, 00-202 Warszawa.

Korekta: Instytut LegalTech przy Naczelnej Radze Adwokackiej.

Skład i łamanie: Instytut LegalTech przy Naczelnej Radze Adwokackiej.

WSTĘP

Wraz z rozwojem technologii cyfrowych, popularyzacją pracy zdalnej i upowszechnieniem narzędzi opartych na sztucznej inteligencji cyberbezpieczeństwo stało się jednym z kluczowych wyzwań współczesnej praktyki adwokackiej, zaś sposób funkcjonowania kancelarii już obecnie uległ głębokiej przemianie i nic nie wskazuje na to, aby ta tendencja miała szybko przeminąć. W tych okolicznościach dbałość o bezpieczeństwo informacji nie jest już kwestią wyboru, lecz stanowi nieodzowny element należytej staranności zawodowej. W tym kontekście szczególnego znaczenia nabiera także standaryzacja *Dobrych praktyk*, budowanie świadomości ich znaczenia oraz kształtowanie trwałych nawyków, które czynią z higieny cybernetycznej naturalną część codziennej pracy prawnika. Dlatego właśnie przedkładamy na ręce Czytelników niniejszy dokument, stanowiący zaktualizowaną wersję *Dobrych Praktyk dotyczących cyberbezpieczeństwa w działalności kancelarii adwokackich i pracy Adwokata* (dalej *Dobre Praktyki*), opracowanych pod patronatem Naczelnej Rady Adwokackiej i opublikowanych pierwotnie w 2022 r.

Drugie wydanie powstało w odpowiedzi na istotne zmiany w krajowych i europejskich regulacjach dotyczących bezpieczeństwa informacji, w tym wejście w życie dyrektywy (UE) 2022/2555 (NIS2), publikację NIST Cybersecurity Framework 2.0 oraz najnowsze wytyczne European Union Agency for Cybersecurity (ENISA). Jednak nawet bez tych zmian taka aktualizacja byłaby konieczna, albowiem rzeczywistość cyfrowa rozwija się szybciej niż jakiegokolwiek regulacje, a konieczność adaptowania się do tak dynamicznego środowiska wymusza nie tyle aktywność legislacyjną, co przede wszystkim oddolna ewolucja zagrożeń i usiłująca za nią nadążyć przemiana społeczna, agregująca zmianę postaw, świadomości i praktyk, które stanowią prawdziwy fundament odporności na ów zagrożenia.

W świecie, w którym tempo rozwoju technologii często przewyższa tempo reakcji instytucji, to właśnie codzienne działania, konsekwencja i uważność użytkowników systemów, w tym odgrywających w nich często szczególnie istotną rolę adwokatów, decydują o realnym poziomie bezpieczeństwa. Współczesne kancelarie funkcjonują w środowisku, w którym granica między sferą technologiczną a prawną coraz bardziej się zaciera, cyberbezpieczeństwo przestaje być domeną informatyków, a staje się codziennym obowiązkiem każdego świadomego beneficjenta technologicznych zdobyczy, zwłaszcza jeśli świadczy on usługi i to niezależnie od profilu działalności. Nowe technologie, takie jak modele przetwarzania w chmurze, czy systemy oparte na sztucznej inteligencji, otwierają przed zawodem ogromne możliwości, ale równocześnie

zwiększają zakres odpowiedzialności za ochronę danych i tajemnicy zawodowej. Celem niniejszego opracowania jest więc dostarczenie adwokatom praktycznych wskazówek służących bezpiecznemu funkcjonowaniu w cyfrowym środowisku pracy. *Dobre Praktyki* nie są zbiorem przepisów ani katalogiem obowiązkowych działań, lecz stanowią narzędzie wspomagające refleksję i rozwój własny, mające pomóc w budowaniu trwałej kultury bezpieczeństwa. Rozwój w obszarze cyberbezpieczeństwa nie jest bowiem celem, który można raz osiągnąć i pozostać biernym w przekonaniu o odporności na wszelkie sygnalizowane ryzyka, aż do momentu publikacji kolejnej edycji *Dobrych Praktyk*. To proces złożony z powtarzających się cykli uczenia się, obserwacji i reagowania, droga nieustannego uwrażliwiania się na zagrożenia i samodoskonalenia. Cyberbezpieczeństwo to dziś zbiór kompetencji i nawyków służących nam w codziennej egzystencji, a więc nie tylko pracy, to zestaw niezbędnych narzędzi, a nie wiedza statyczna. Dlatego niniejszy dokument nie aspiruje do wyczerpania prezentowanego zagadnienia, tym bardziej, iż starania te mogłyby przynieść odwrotny skutek, czyniąc omawiane treści trudniejszymi do przyswojenia. Tym samym należy stanowczo zaznaczyć, iż stosowanie *Dobrych Praktyk* nie może ograniczać się do samego formalnego wdrożenia zalecanych polityk, lecz musi wiązać się z trwałą zmianą sposobu w jaki zwykło się niekiedy postrzegać wykonywanie zawodu adwokata, w tym jako zawód „nietechniczny”, który jako taki miałyby być zwolniony z obowiązku rozwoju w obszarach dotychczas niekojarzonych z praktyką prawniczą.

Wobec powyższego, mając na uwadze szczególnie charakter zawodów zaufania publicznego, a w szczególności zawodu adwokata, należy przyjąć, że praktyki, o których traktuje niniejszy dokument, nie są już obszarem fakultatywnym ani przejawem trendu, lecz stanowią wyraz zawodowej odpowiedzialności i obowiązku każdego adwokata wobec klientów, współpracowników oraz całego środowiska prawniczego. Wymagają one jednak nie tylko znajomości zasad i procedur, lecz także zdolności do krytycznej refleksji nad własnymi przyzwyczajeniami, postawami i decyzjami, które często same stają się źródłem zagrożeń w cyfrowym świecie. Wszakże konfrontując się z wyzwaniem cyberzagrożeń, konfrontujemy się niejako z kolejnym przejawem własnych skłonności i słabości, któremu nie może towarzyszyć lęk przed tym, co zobaczymy, lecz gotowość potraktowania tego doświadczenia jako impulsu do dalszego rozwoju, zarówno zawodowego jak i osobistego oraz do stawania się bardziej świadomymi, odpowiedzialnymi i odpornymi uczestnikami świata, który sami współtworzymy.

Członkowie grupy roboczej wydania II.

*Dobrych Praktyk dotyczących cyberbezpieczeństwa
w działalności kancelarii adwokackich i pracy adwokata*

WYTYCZNE I ZALECENIA ZOSTAŁY OPRACOWANE WE WSPÓŁPRACY:



INSTYTUT
LEGALTECH NRA

Wydanie I - 2022 r.

Instytutu LegalTech przy Naczelnej Radzie Adwokackiej

Zespół ds. dobrych praktyk dotyczących cyberbezpieczeństwa Instytutu LegalTech przy Naczelnej Radzie Adwokackiej:

- adw. Przemysław Barchan - Dyrektor Instytutu LegalTech przy Naczelnej Radzie Adwokackiej
- adw. Adam Baworowski - Członek Instytutu LegalTech przy Naczelnej Radzie Adwokackiej
- adw. Paulina Rzeszut - Wicedyrektor Instytutu LegalTech przy Naczelnej Radzie Adwokackiej
- adw. Piotr Warchoł - Wicedyrektor Instytutu LegalTech przy Naczelnej Radzie Adwokackiej

Wydanie II - 2025 r.

Instytutu LegalTech przy Naczelnej Radzie Adwokackiej, w tym:

- adw. Oskar Grajewski – Koordynator prac grupy roboczej wydania II. *Dobrych Praktyk*, Członek Instytutu LegalTech przy Naczelnej Radzie Adwokackiej
- adw. Paulina Rzeszut – Dyrektor Instytutu LegalTech przy Naczelnej Radzie Adwokackiej
- adw. Mikołaj Śniatała – Wicedyrektor Instytutu LegalTech przy Naczelnej Radzie Adwokackiej
- adw. Aleksandra Ostręga – Członek Instytutu LegalTech przy Naczelnej Radzie Adwokackiej
- adw. Magdalena Stec – Członek Instytutu LegalTech przy Naczelnej Radzie Adwokackiej
- adw. Jabuk Derulski – Członek Instytutu LegalTech przy Naczelnej Radzie Adwokackiej
- adw. Marcin Barczyk – Członek Instytutu LegalTech przy Naczelnej Radzie Adwokackiej
- adw. Zbigniew Bakalarczyk – Członek Instytutu LegalTech przy Naczelnej Radzie Adwokackiej



Komisji Nowych Technologii i Informatyzacji przy Wielkopolskiej Izbie Adwokackiej, w tym:

- adw. Arkadiusz Habiera – Członek Komisja Nowych Technologii i Informatyzacji przy Wielkopolskiej Izbie Adwokackiej
- adw. Andrzej J. Reichelt – Członek Komisja Nowych Technologii i Informatyzacji przy Wielkopolskiej Izbie Adwokackiej

Spis treści

WPROWADZENIE	4
METODOLOGIA	6
DEFINICJE	10
ROZDZIAŁ I. ZALECENIA PODSTAWOWE	13
1. <i>Zalecenia ogólne.....</i>	13
2. <i>Komputery PC i przenośne</i>	15
3. <i>Smartfon</i>	16
4. <i>Serwery i urządzenia NAS</i>	17
5. <i>Komunikacja w sieci Internet / sieć.....</i>	18
6. <i>Poczta elektroniczna.....</i>	19
7. <i>Back-up.....</i>	20
8. <i>Przetwarzanie danych w Usługach Online.....</i>	20
9. <i>Przekazywanie danych poza Kancelarię, w tym do klienta</i>	21
10. <i>Biura serwisowane</i>	22
11. <i>Komunikatory.....</i>	22
12. <i>Obsługa zewnętrzna IT</i>	23
13. <i>Reagowanie na incydenty</i>	23
14. <i>Praca Zdalna i Mobilna</i>	24
ROZDZIAŁ II. ZALECENIA DODATKOWE	25
15. <i>Zalecenia ogólne.....</i>	26
16. <i>Komputery PC i przenośne</i>	28
17. <i>Smartfon</i>	28
18. <i>Serwery i urządzenia NAS.....</i>	29
19. <i>Poczta elektroniczna</i>	29
20. <i>Back-up.....</i>	29
21. <i>Przetwarzanie danych w Usługach Online.....</i>	29
22. <i>Przekazywanie danych poza Kancelarię, w tym do klienta.....</i>	30
23. <i>Obsługa zewnętrzna IT.....</i>	30
24. <i>Reagowanie na Incydenty</i>	30
25. <i>Praca zdalna i mobilna</i>	30
ZAŁĄCZNIK NUMER 1 DO DOBRZYCH PRAKTYK DOTYCZĄCYCH CYBERBEZPIECZEŃSTWA W DZIAŁALNOŚCI KANCELARII ADWOKACKICH I PRACY ADWOKATA	32
ROZDZIAŁ I. ZALECENIA PODSTAWOWE	32
ROZDZIAŁ II. ZALECENIA DODATKOWE	51
ZAŁĄCZNIK NUMER 2 DO DOBRZYCH PRAKTYK DOTYCZĄCYCH CYBERBEZPIECZEŃSTWA W DZIAŁALNOŚCI KANCELARII ADWOKACKICH I PRACY ADWOKATA	61
ZALECENIA DODATKOWE KWARTALNY SELF-CHECK BEZPIECZEŃSTWA PRACY ZDALNEJ	61
LISTA KONTROLNA WIDEO-ROZPRAW/SPOTKAŃ ONLINE.....	62
ZAŁĄCZNIK NUMER 3 DO DOBRZYCH PRAKTYK DOTYCZĄCYCH CYBERBEZPIECZEŃSTWA W DZIAŁALNOŚCI KANCELARII ADWOKACKICH I PRACY ADWOKATA	63
LISTA KONTROLNA BEZPIECZEŃSTWA DOSTAWCY IT	63
ZAŁĄCZNIK NUMER 4 DO DOBRZYCH PRAKTYK DOTYCZĄCYCH CYBERBEZPIECZEŃSTWA W DZIAŁALNOŚCI KANCELARII ADWOKACKICH I PRACY ADWOKATA	65
NARZĘDZIE WSPIERAJĄCE ZASADĘ NALEŻYTEJ STARANNOŚCI I PODEJŚCIE OPARTE NA RYZYKU	65

WPROWADZENIE

Dobre Praktyki mają charakter zaleceń, których stosowanie nie jest obligatoryjne a brak ich stosowania nie rodzi bezpośrednich negatywnych skutków w odpowiedzialności zawodowej czy dyscyplinarnej, lecz nie zmienia to faktu, iż istotna ich część już obecnie koreluje z obowiązkami wynikającymi z przepisów prawa i z norm etycznych przystosowanych do zawodu adwokata, a zatem nie jest wykluczone, iż zaniechanie ich wdrożenia i stosowania może w pewnych przypadkach prowadzić do takiej odpowiedzialności w sposób pośredni. Sam fakt fakultatywności zaleceń nie wyłącza także obowiązków adresatów *Dobrych Praktyk* w zakresie dołożenia należytej staranności w dochowaniu tajemnicy zawodowej, określonych przepisami prawa i aktów samorządu adwokackiego, w szczególności regulujących zasady etyki zawodowej adwokata i godności zawodu. Przedstawione w niniejszym dokumencie praktyki nie stanowią wyczerpującej listy zaleceń z zakresu cyberbezpieczeństwa, a raczej pełnią funkcję przewodnika po zasadach i procedurach umożliwiających utrzymanie wysokiego poziomu bezpieczeństwa informacji w realiach nowoczesnej kancelarii i mają one charakter swoistego wsparcia merytorycznego, które winno ułatwić wdrażanie w codzienną działalność kancelarii zasad dotyczących ochrony danych oraz cyberbezpieczeństwa. Kancelarie, w tym adwokaci prowadzący indywidualną praktykę zawodową, powinni dołożyć należytej staranności w doborze środków technicznych i organizacyjnych pozwalających na utrzymanie właściwych zabezpieczeń teleinformatycznych i ich stosowaniu. W przypadkach, w których Adwokat nie posiada wystarczającej wiedzy teleinformatycznej i z zakresu cyberbezpieczeństwa zaleca się korzystnie z usług specjalistycznych podmiotów trzecich. Kancelarie posiadające Personel mogą rozważyć zasadność włączenia do jego składu odpowiednich specjalistów. Rekomendacje zawarte w przedmiotowym dokumencie nie zawierają wytycznych w zakresie stosowania narzędzi i technologii pochodzących od określonych producentów i dostawców. Przedstawienie w *Dobrych Praktykach* przykładów narzędzi byłoby niewskazane z uwagi na charakter *Dobrych Praktyk*, a także brak możliwości przeprowadzania systematycznej analizy poszczególnych narzędzi w celu podtrzymania ww. rekomendacji.

Mając powyższe na uwadze, stosowanie *Dobrych Praktyk* nie gwarantuje pewności ochrony przed Incydentami i nie zwalnia Kancelarii i danego Adwokata z odpowiedzialności za

dochowanie należytej staranności w zapewnieniu bezpieczeństwa w powyższym zakresie.

Adresaci *Dobrych Praktyk* powinni dokonać zmapowania procesów i zabezpieczeń stosowanych wewnątrz własnej organizacji, a następnie – w oparciu o rzetelną analizę ryzyka – podjąć decyzję w przedmiocie stosowania określonych środków technicznych i organizacyjnych, w tym poszczególnych zaleceń zawartych w *Dobrych Praktykach*. Jeśli w oparciu o ww. analizę, a także specyfikę przetwarzanych danych, stosowanie określonych zaleceń nie byłoby właściwe, Kancelaria lub dany Adwokat powinien pominąć dane zalecenia. Zakres *wdrożenia Dobrych Praktyk* powinien być przy tym proporcjonalny do skali i charakteru działalności Kancelarii. W przypadku mniejszych kancelarii wystarczające może być zastosowanie podstawowych środków ochrony, natomiast kancelarie średnie i duże powinny rozważyć wdrożenie bardziej zaawansowanych procedur zarządzania bezpieczeństwem informacji, w tym okresowych audytów i szkoleń personelu. *Dobre Praktyki* nie stanowią również wytycznych w zakresie dochowania przez Kancelarię i Adwokata zgodności przetwarzania przez nich danych osobowych z stosownymi przepisami prawa, w tym rozporządzeniem 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. W szczególności, z uwagi na obowiązki określone powyższymi przepisami, konieczne może być przyjęcie wyższych standardów ochrony danych niż wskazane w niniejszym dokumencie. Na *Dobre Praktyki* składają się zalecenia przedstawione w głównej części w formie tabel pogrupowanych według pól tematycznych (m.in. technologicznych, procesowych) wraz z ich rozróżnieniem na adresatów zawartych zaleceń, a także załącznik zawierający omówienie poszczególnych zaleceń. Główna część podzielona jest na wprowadzenie, rozdział I (zawierający zalecenia podstawowe dla wszystkich adresatów, w tym Kancelarii jednoosobowych) oraz rozdział II (zawierający zalecenia dodatkowe, przeznaczone dla pozostałych grup Kancelarii).

Dobre Praktyki należy traktować jako dokument otwarty, podlegający aktualizacjom wraz ze zmianami środowiska prawnego, technologicznego i organizacyjnego. Ich skuteczność zależy nie od samego wdrożenia, lecz od utrzymywania ciągłego procesu doskonalenia i wymiany doświadczeń w środowisku zawodowym.

METODOLOGIA

Przy opracowywaniu niniejszych *Dobrych Praktyk* przyjęto podejście oparte na zasadzie proporcjonalności. Oznacza to, że zakres i sposób wdrożenia środków bezpieczeństwa powinny odpowiadać skali działalności, poziomowi ryzyka, rodzajowi przetwarzanych informacji oraz możliwościom organizacyjnym i technicznym danej Kancelarii. Celem przyjętej metodologii nie jest sztywna klasyfikacja kancelarii, lecz ułatwienie dopasowania środków ochrony do ich faktycznych potrzeb i zasobów. Różnice w liczbie personelu, infrastrukturze technicznej oraz strukturze organizacyjnej mają bowiem istotny wpływ na zakres obowiązków i odpowiedzialności w obszarze bezpieczeństwa informacji. W tym celu przyjęto podział na cztery grupy kancelarii, od jednoosobowych po duże podmioty, odzwierciedlający zróżnicowanie poziomu ryzyka i dostępnych środków technicznych, organizacyjnych oraz procesowych. Poniższe zestawienie ma charakter orientacyjny i stanowi punkt odniesienia dla doboru adekwatnych praktyk i zabezpieczeń, przy czym każda Kancelaria powinna w pierwszej kolejności przeprowadzić własną analizę ryzyka i w oparciu o jej wyniki dostosować zakres wdrożenia *Dobrych Praktyk*.

GRUPA	OPIS
jednoosobowe (1-os.)	Adwokaci prowadzący kancelarie w formie jednoosobowych działalności gospodarczych, którzy swoją praktykę prowadzą samodzielnie, tj. bez zatrudniania stałego Personelu kancelarii. Przez zatrudnienie stałego Personelu należy rozumieć zawarcie z daną osobą umowy o pracę lub umów cywilnoprawnych, w tym umowy o współpracę z osobą prowadzącą jednoosobową działalność gospodarczą, jeśli z umowy i praktyki wynika, że osoby te pełnią rolę stałych pracowników lub współpracowników Kancelarii. Osoby współpracujące z Kancelarią jako niezależny zewnętrzny współpracownik (np. <i>of Counsel</i>) powinny być traktowane jako osoba trzecia, z którą należy zawrzeć odpowiednie umowy lub udzielić stosownych upoważnień.
Małe (2 – 10 os.)	Kancelarie adwokackie prowadzone w dowolnej formie prawnej (jednoosobowe działalności gospodarcze, zespoły adwokackie, spółki osobowe), których skład osobowy (wspólników i Personelu) mieści się między 2 a 10 osób. Przez zatrudnienie stałego Personelu należy rozumieć zawarcie z daną osobą umowy o pracę lub umów cywilnoprawnych, w tym umowy o współpracę z osobą prowadzącą jednoosobową działalność gospodarczą, jeśli z umowy i praktyki wynika, że osoby te pełnią rolę stałych pracowników lub współpracowników

	Kancelarii. Osoby współpracujące z Kancelarią jako niezależny zewnętrzny współpracownik (np. <i>of Counsel</i>) powinny być traktowane jako osoba trzecia, z którą należy zawrzeć odpowiednie umowy lub udzielić stosownych upoważnień.
Średnie (11 – 20 os.)	Kancelarie adwokackie prowadzone w dowolnej formie prawnej (jednoosobowe działalności gospodarcze, zespoły adwokackie, spółki osobowe), których skład osobowy (wspólników i Personelu) mieści się między 11 a 20 osób. Przez zatrudnienie stałego Personelu należy rozumieć zawarcie z daną osobą umowy o pracę lub umów cywilnoprawnych, w tym umowy o współpracę z osobą prowadzącą jednoosobową działalność gospodarczą, jeśli z umowy i praktyki wynika, że osoby te pełnią rolę stałych pracowników lub współpracowników Kancelarii. Osoby współpracujące z Kancelarią jako niezależny zewnętrzny współpracownik (np. <i>of Counsel</i>) powinny być traktowane jako osoba trzecia, z którą należy zawrzeć odpowiednie umowy lub udzielić stosownych upoważnień. Kancelaria taka powinna korzystać z usług wsparcia IT, celem odpowiedniego zabezpieczenia informacji.
Duże (powyżej 20 os.)	Kancelarie adwokackie prowadzone w dowolnej formie prawnej (jednoosobowe działalności gospodarcze, zespoły adwokackie, spółki osobowe), których skład osobowy (wspólników i personelu) wynosi powyżej 20 osób. Przez zatrudnienie stałego Personelu należy rozumieć zawarcie z daną osobą umowy o pracę lub umów cywilnoprawnych, w tym umowy o współpracę z osobą prowadzącą jednoosobową działalność gospodarczą, jeśli z umowy i praktyki wynika, że osoby te pełnią rolę stałych pracowników lub współpracowników Kancelarii. Osoby współpracujące z Kancelarią jako niezależny zewnętrzny współpracownik (np. <i>of Counsel</i>) powinny być traktowane jako osoba trzecia, z którą należy zawrzeć odpowiednie umowy lub udzielić stosownych upoważnień. Kancelaria taka powinna korzystać z usług IT, celem odpowiedniego zabezpieczenia informacji.

Dobre Praktyki stosuje się odpowiednio do aplikantów adwokackich oraz prawników zagranicznych wpisanych na listę prawników zagranicznych prowadzoną przez właściwą okręgową radę adwokacką, z zastrzeżeniem, że odpowiedzialność nad stosowaniem właściwych *Dobrych Praktyk* z zakresu cyberbezpieczeństwa w przypadku:

- a) aplikanta adwokackiego będącego członkiem Personelu – ponosi Kancelaria,
- b) aplikanta adwokackiego prowadzącego jednoosobową działalność gospodarczą i świadczącego swoje usługi poza ramami stosunku prawnego członka Personelu – ponosi sam aplikant adwokacki w zakresie przewidzianym umową lub upoważnieniem.

Dobre Praktyki stosuje się również (w stopniu właściwym dla Kancelarii 1-osobowych) do Adwokatów i aplikantów adwokackich prowadzących jednoosobową działalność gospodarczą współpracujących z podmiotami gospodarczymi lub instytucjami w charakterze prawnika in-house, w zakresie w jakim korzystają oni ze sprzętu lub infrastruktury informatycznej takiego podmiotu gospodarczego lub instytucji. Głównym zaleceniem w ich przypadku jest jednak poinformowanie ww. podmiotów lub instytucji o istnieniu *Dobrych Praktyk*, a także podjęcie próby uwzględnienia *Dobrych Praktyk* w ochronie przed Incydentami w ramach możliwości technicznych, i organizacyjnych udostępnionych przez ww. podmiot lub instytucję.

Dobre Praktyki mają zastosowanie do Kancelarii małych, średnich i dużych prowadzonych w formie spółek osobowych, w których współnikami są również inne niż Adwokaci osoby wykonujące zawody określone w art. 4a ust. 1 ustawy z dnia 26 maja 1982 roku – Prawo o adwokaturze (j.t.: Dz.U. z 2020 r., poz. 1651 ze zm.).

Z uwagi na poruszaną w *Dobrych Praktykach* materię, dokument ten będzie podlegał okresowym przeglądom i zmianom, z zastrzeżeniem, że mając na uwadze krótki cykl zmian technologicznych oraz wzrastający poziom zagrożenia Incydentami, utrzymanie aktualnego charakteru zwartych w nim zaleceń może nie być możliwe. Rekomendowane jest zatem regularne śledzenie aktualnych zaleceń instytucji zajmujących się tematyką cyberbezpieczeństwa (np. ENISA¹).

Podsumowując, zalecane jest stosowanie przez Adwokatów i Kancelarie środków technicznych, organizacyjnych i procesowych właściwych dla zapewnienia odpowiedniej ochrony danych objętych Tajemnicą zawodową, danych osobowych i pozostałych informacji prawnie chronionych znajdujących się w posiadaniu adwokata i Kancelarii, przed ich ujawnieniem w wyniku Incydentu.

Na *Dobre Praktyki* składają się zalecenia przedstawione poniżej w formie tabel pogrupowanych według obszarów tematycznych (m.in. technologicznych, procesowych) wraz z ich rozróżnieniem na adresatów zawartych zaleceń.

¹ *European Union Agency for Cybersecurity* (Agencja Unii Europejskiej ds. Cyberbezpieczeństwa).

Poszczególne zalecenia uwzględnione w tabelach zostały oznaczone przy adresatach jako:

- | | | |
|--|------------------------|----|
| ➤ zalecane opcjonalnie (dobrą praktyką jest stosowanie danego zalecenia, ale z uwagi na wielkość Kancelarii, możliwości organizacyjne, techniczne i budżet, realizacja może utrudnić funkcjonowanie Kancelarii bez istotnej poprawy poziomu bezpieczeństwa), | zalecane
opcjonalne | ZO |
| ➤ zalecane (dobrą praktyką jest stosowanie danego zalecenia), | zalecane | Z |
| ➤ niezalecane (dobrą praktyką jest powstrzymanie się od stosowania określonych czynności, realizacji określonego sposobu działania lub poddania się wpływowi określonych czynników/zdarzeń, które stanowią stan niepożądany z perspektywy bezpieczeństwa Kancelarii i jej środowiska informatycznego). | niezalecane | N |

Poniższy rozdział I określa zalecenia podstawowe dla wszystkich grup Kancelarii, a w szczególności dedykowane Kancelariom jednoosobowym. Rozdział II określa zalecenia uzupełniające rozdział I o zalecenia przeznaczone dla Kancelarii małych, średnich i dużych, którym wskazuje się stosowanie również do zaleceń określonych w rozdziale I. Kancelarie jednoosobowe mogą stosować się również do zaleceń określonych w rozdziale II, w zależności od wyników oceny ryzyka naruszenia przetwarzania informacji.

DEFINICJE

Pojęcia wykorzystane w niniejszych *Dobrych Praktykach* wielką literą powinny być rozumiane zgodnie z poniższymi definicjami (niezależnie od wykorzystania ich w formie pojedynczej lub mnogiej):

Checklista Weryfikacji Dostawcy	sformalizowany zbiór kryteriów i pytań (lista kontrolna) służący do przeprowadzenia audytu bezpieczeństwa i oceny ryzyka związanego z nawiązaniem współpracy z nowym dostawcą usług online. Checklista powinna obejmować weryfikację aspektów technicznych (np. stosowane szyfrowanie, dostępność MFA), organizacyjnych (np. certyfikaty ISO) oraz prawnych (np. lokalizacja danych na terytorium EOG, treść umowy DPA, klauzule poufności).
Chmura Obliczeniowa	pula 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. Chmura Obliczeniowa dostarczana jest z reguły w 3 modelach usługowych (SaaS, PaaS, IaaS) i 4 modelach wdrożenia (chmura prywatna, publiczna, społecznościowa i hybrydowa). ²
Dobre Praktyki	niniejsze <i>Dobre Praktyki</i> dotyczące cyberbezpieczeństwa w działalności Kancelarii i pracy Adwokata.
Dostawca Usług Chmurowych	podmiot, który dysponuje infrastrukturą i oprogramowaniem służącym do świadczenia Usług Chmurowych oraz świadczy te usługi.
Dostawca Usług Online	podmiot, który prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową świadczy Usługi Online. Dostawcą Usług Online jest w szczególności Dostawca Usług Chmurowych.
DPA	umowa powierzenia przetwarzania danych osobowych, w tym zawierana poprzez akceptację regulaminu lub polityki przetwarzania danych osobowych dostawcy.
EFTA	Europejskie Stowarzyszenie Wolnego Handlu.
EOG	Europejski Obszar Gospodarczy.

Hasło administratora	hasło umożliwiające pełne zarządzanie systemem informatycznym, w tym nadawanie i odbieranie uprawnień poszczególnym użytkownikom.
Kancelaria	organizacja służąca wykonywaniu zawodu przez Adwokata, prowadzona w formie przewidzianej przepisami prawa (jednoosobowa działalność gospodarcza, zespół adwokacki, spółka osobowa).
Klient poczty	aplikacja na urządzenie mobilne lub komputer stacjonarny służąca do obsługi korespondencji e-mail.
Incydent	pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
Personel	zespół Kancelarii złożony z osób zatrudnionych w Kancelarii na podstawie umowy o pracę lub umów cywilnoprawnych, w tym umów o współpracę zawartymi z osobami prowadzącymi działalność gospodarczą w formie jednoosobowej działalności gospodarczej (będącymi stałymi członkami zespołu Kancelarii a nie zewnętrznymi współpracownikami).
RODO	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.
SaaS	oprogramowanie jako usługa – model usługi chmurowej umożliwiający odbiorcy usług wykorzystanie aplikacji uruchomionych na infrastrukturze chmury dostarczanej przez dostawcę usług dostępnej na różnych urządzeniach klienckich za pośrednictwem np. przeglądarki internetowej lub klienta aplikacji oraz w przypadku której odbiorca usług nie zarządza ani nie kontroluje infrastruktury chmury, w tym sieci, serwerów, systemów operacyjnych, pamięci masowej, a nawet parametrów konfiguracyjnych aplikacji, z wyjątkiem ograniczonych ustawień konfiguracji aplikacji specyficznych dla użytkownika. ⁴
Szyfrowanie <i>at rest</i>	szyfrowanie danych „w spoczynku” (np. szyfrowanie przechowywanych plików, kopii zapasowych, informacji zgromadzonych w bazie danych).

Szyfrowanie <i>in transit</i>	szyfrowanie danych w trakcie transmisji (przesyłania) danych (np. podczas przesyłania danych w sieci teleinformatycznej, w tym z/do Chmury Obliczeniowej).
Tajemnica zawodowa	tajemnica zawodowa w rozumieniu art. 6 ustawy z dnia 26 maja 1982 roku – Prawo o adwokaturze (j.t.: Dz.U. z 2020 r., poz. 1651 ze zm.), obejmująca w szczególności tajemnicę obrończą.
UK	Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej, z wyłączeniem terytoriów zależnych.
Usługi Chmurowe	gotowe do użycia, wystandaryzowane zasoby Chmury Obliczeniowej służące przetwarzaniu informacji, wstępnie skonfigurowane przez Dostawcę Usług Chmurowych i przez niego dostarczane. Usługi Chmurowe mogą być bezpośrednio dostarczane Kancelarii lub stanowić element usług innego dostawcy.
Usługi Online	usługi świadczone drogą elektroniczną, 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. Usługami Online są w szczególności Usługi Chmurowe.
VPN	Virtual Private Network, czyli wirtualna sieć prywatna. Jest to technologia, która umożliwia bezpieczne i szyfrowane połączenie między urządzeniem użytkownika (np. komputerem, smartfonem) a serwerem VPN w Internecie. Dzięki temu dane przesyłane przez sieć są chronione przed nieuprawnionym dostępem, podsłuchem czy ingerencją osób trzecich.

² Za National Institute of Standards and Technology, *Definition of Cloud Computing*, NIST Special Publication 800-145, Gaithersburg, MD: U.S. Department of Commerce, September 2011 [protokół dostępu: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf] [data dostępu: 9 października 2025 r.].

³ Za National Institute of Standards and Technology, *Definition of security incident*, NIST Special Publication 800-128, Gaithersburg, MD: U.S. Department of Commerce, September 2011 [protokół dostępu: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf] [data dostępu: 9 października 2025 r.].

⁴ Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” (M.P. z 2019 r. poz. 862).

ROZDZIAŁ I. ZALECENIA PODSTAWOWE

dedykowane dla Kancelarii jednoosobowych, bazowe dla pozostałych grup Kancelarii

Poniższe zalecenia są zaleceniami minimalnymi, powalającymi na zwiększenie bezpieczeństwa Tajemnicy zawodowej w świecie cyfrowym. W zależności od wiedzy, posiadanych umiejętności i wyników własnej oceny ryzyka przetwarzania informacji Adwokat może stosować wyższe standardy zabezpieczeń, w tym zalecenia dodatkowe wskazane w Rozdziale II.

1. Zalecenia ogólne

Numer Zalecenia	Czynnik \ Adresat	1 os.
1.1	Korzystanie wyłącznie z licencjonowanego, aktualnego i wspieranego przez producenta oprogramowania przeznaczonego do komercyjnego zastosowania, z włączonym automatycznym systemem aktualizacji bezpieczeństwa. Regularne (co najmniej kwartalne) sprawdzanie i aktualizacja systemów operacyjnych, aplikacji oraz oprogramowania sprzętowego (firmware).	Z
1.2	W przypadku korzystania z aplikacji lub usług, w ramach których dostawcy uzyskują dostęp do danych osobowych przetwarzanych przez Kancelarię, zawarcie stosownej DPA, zgodnej z przepisami RODO i zasadami dostępu do Tajemnicy zawodowej, obejmującej m.in.: obowiązek zgłaszania incydentów, zasady korzystania z podprocesorów, lokalizację danych oraz obowiązek szyfrowania transmisji i przechowywania.	Z
1.3	Korzystanie z rozwiązań i usług informatycznych tylko od zaufanych dostawców, posiadających siedzibę na terytorium EOG, którzy umożliwiają (gdy dochodzi do powierzenia przetwarzania danych osobowych) zawarcie stosownej DPA, a także przetwarzających powierzone dane na terytorium EOG. Przed rozpoczęciem korzystania z usług dostawcy przeprowadzenie wstępnej oceny bezpieczeństwa dostawcy (checklisty lub ankiety bezpieczeństwa) oraz coroczny przegląd zgodności (np. certyfikaty ISO 27001, raport SOC2, audyt zewnętrzny). Monitorowanie zmian w relacjach z dostawcami, w tym podprocesorów, lokalizacji danych, polityk prywatności oraz zgłoszonych incydentów bezpieczeństwa.	Z

1.4	Zapewnienie fizycznych zabezpieczeń miejsc przechowywania sprzętu i nośników danych, w tym kontroli dostępu, stosowania zamków, systemów alarmowych, monitoringu oraz zabezpieczenia urządzeń przed nieuprawnionym dostępem. W przypadku przechowywania lub transportu nośników danych obowiązkowe jest szyfrowanie danych oraz stosowanie ewidencji wydania i zwrotu nośników.	Z
1.5	Korzystanie ze sprzętu należącego do osób trzecich, w szczególności przy dostępie do informacji objętych Tajemnicą zawodową. W przypadku pracy zdalnej dopuszczalne jest korzystanie wyłącznie ze sprzętu służbowego lub zatwierdzonego przez Kancelarię, zabezpieczonego systemem szyfrowania dysku, aktualnym oprogramowaniem i połączeniem VPN.	N
1.6	Okresowy przegląd cyberzagrożeń i dostosowanie stosownych środków technicznych i organizacyjnych przy uwzględnieniu istniejących i potencjalnych ryzyk. Przegląd ryzyk powinien być przeprowadzany co najmniej raz w roku oraz po każdym istotnym incydencie. Wyniki powinny być dokumentowane w Rejestrze Ryzyk lub Raporcie z Analizy Ryzyka. Powinien też zostać wdrożony i być utrzymywany uproszczonego Planu Reagowania na Incydenty (Incident Response Plan), określający role, sposób zgłaszania i dokumentowania incydentów.	Z
1.7	Regularne szkolenia w zakresie wdrożonych polityk bezpieczeństwa i zasad korzystania ze sprzętu i usług. Szkolenia powinny być prowadzone przy rozpoczęciu współpracy i nie rzadziej niż raz w roku, z dokumentowaniem uczestnictwa. Zaleca się prowadzenie ćwiczeń praktycznych (np. symulacji phishingu) oraz krótkich testów wiedzy w ramach utrwalania świadomości bezpieczeństwa.	Z
1.8	Posiadanie ubezpieczenia w zakresie odpowiedzialności dotyczącej cyberbezpieczeństwa i RODO. Ubezpieczenie powinno obejmować w szczególności koszty reakcji na incydent, odzyskiwania danych, odpowiedzialność za naruszenie ochrony danych osobowych oraz straty finansowe klientów.	ZO
1.9	Dokumenty elektroniczne i pliki przesyłane na zewnątrz powinny być pozbawiane metadanych (EXIF, DOCX, PDF). Powinna zostać wprowadzona polityka retencji i niszczenia danych.	Z
1.10	Wprowadzanie danych objętych tajemnicą zawodową do publicznych lub nieautoryzowanych systemów sztucznej inteligencji.	N
1.11	W przypadku wykorzystywania narzędzi opartych na AI – obowiązek uprzedniej weryfikacji bezpieczeństwa i poufności oraz dokumentowania zapytań (promptów) i wyników.	Z

1.12	Każde działanie związane z wdrażaniem nowych technologii, usług online lub zmian w procesach kancelarii powinno uwzględniać zasadę Security & Privacy by Design, tj. projektowanie rozwiązań z uwzględnieniem bezpieczeństwa informacji i ochrony danych osobowych od samego początku. W praktyce oznacza to, że przed wdrożeniem nowego narzędzia lub procedury należy dokonać oceny potencjalnych ryzyk dla bezpieczeństwa i prywatności, określić minimalny zestaw środków ochrony oraz zapewnić zgodność z zasadami tajemnicy zawodowej i przepisami o ochronie danych osobowych, w szczególności z RODO.	Z
------	---	---

2. Komputery PC i przenośne

Numer Zalecenia	Czynnik \ Adresat	1 os.
2.1	Stosowanie silnych haseł dostępowych.	Z
2.2	Stosowanie jednego hasła do kilku kont dostępowych.	N
2.3	Przeprowadzanie okresowej zmiany haseł lub stosowanie menadżera haseł.	Z
2.4	Stosowanie uwierzytelniania wieloskładnikowego (MFA).	Z
2.5	Stosowanie szyfrowania danych i komunikacji.	Z
2.6	Stosowanie darmowego oprogramowania antywirusowego przeznaczonego do użytku osobistego.	N
2.7	Stosowanie oprogramowania antywirusowego w standardzie biznesowym z rozbudowanymi modułami zapory sieciowej i ochroną korespondencji e-mail.	Z
2.8	Wykonywanie okresowych kopii zapasowych systemu operacyjnego i danych.	Z
2.9	Utrzymanie stałej kontroli nad wykorzystywanym sprzętem.	Z
2.10	Stosowanie wygaszacza ekranu zabezpieczonego hasłem.	Z
2.11	Korzystanie z oprogramowania umożliwiającego zdalne zablokowanie dostępu lub usunięcie danych ze sprzętu w przypadku zgubienia lub kradzieży sprzętu.	Z
2.12	Korzystanie z prywatnego sprzętu w celach zawodowych.	N
2.13	Korzystanie w celach zawodowych wyłącznie ze sprzętu służbowego.	Z

2.14	Udostępnianie sprzętu osobie trzeciej (w tym członkowi rodziny) do korzystania.	N
2.15	Korzystanie z zewnętrznego serwisu IT (świadczonego przez podmiot nie zweryfikowany w zakresie bezpieczeństwa informacji) w formie zdalnej bez bieżącego nadzoru, w szczególności w celu naprawy.	N
2.16	Ograniczenie lub wyłączenie działania w tle aplikacji i standardów komunikacji (np. bluetooth i wi-fi), które nie są wykorzystywane w sposób stały i konieczny.	Z
2.17	Dbanie o warunki pracy nie pozwalające na zapoznanie się przez osoby postronne z informacjami wyświetlanymi na ekranie.	Z

3. Smartfon

Numer Zalecenia	Czynnik \ Adresat	1 os.
3.1	Stosowanie silnych haseł dostępowych.	Z
3.2	Stosowanie jednego hasła do kilku kont dostępowych.	N
3.3	Przeprowadzanie okresowej zmiany haseł lub stosowanie menadżera haseł.	Z
3.4	Stosowanie uwierzytelniania wieloskładnikowego (MFA).	Z
3.5	Stosowanie szyfrowania danych i komunikacji.	Z
3.6	Stosowanie darmowego oprogramowania antywirusowego przeznaczonego do użytku osobistego.	N
3.7	Stosowanie oprogramowania antywirusowego w standardzie biznesowym.	Z
3.8	Wykonywanie okresowych kopii zapasowych danych na urządzeniu zewnętrznym.	Z
3.9	Wykonywanie okresowych kopii zapasowych danych objętych Tajemnicą zawodową w Usługach Online producenta sprzętu lub operatora telekomunikacyjnego.	N
3.10	Utrzymanie stałej kontroli nad wykorzystywanym sprzętem.	Z
3.11	Korzystanie z oprogramowania umożliwiającego zdalne zablokowanie dostępu lub usunięcie danych ze sprzętu w przypadku zgubienia lub kradzieży sprzętu.	Z

3.12	Korzystanie z prywatnego sprzętu w celach zawodowych.	N
3.13	Korzystanie w celach zawodowych wyłącznie ze sprzętu służbowego.	Z
3.14	Udostępnianie sprzętu osobie trzeciej (w tym członkowi rodziny) do korzystania.	N
3.15	Ograniczenie lub wyłączenie działania w tle aplikacji i standardów komunikacji (np. Bluetooth, NFC, Wi-Fi).	Z
3.16	Korzystanie z usług telekomunikacyjnych, których abonentem nie jest Kancelaria.	N
3.17	Stosowanie systemów zarządzania urządzeniami mobilnymi (MDM/MAM) dla wszystkich smartfonów służbowych, w tym kontroli aktualizacji, blokady instalacji aplikacji spoza sklepu, możliwości zdalnego wymazania danych i audytu bezpieczeństwa.	Z
3.18	Korzystanie wyłącznie z komunikatorów biznesowych zapewniających szyfrowanie typu E2EE; dopuszczalne wyłącznie aplikacje znajdujące się na białej liście kancelarii (np. Signal, Threema, Wire, MS Teams E2EE).	Z
3.19	Domowe sieci Wi-Fi wykorzystywane do celów zawodowych muszą posiadać standard szyfrowania WPA3, odrębną sieć gościnną oraz zakaz współdzielenia z urządzeniami IoT (inteligentne TV, kamery, AGD).	Z
3.20	Wykonywanie krótkich samoocen bezpieczeństwa (self-check) urządzeń mobilnych nie rzadziej niż raz na kwartał, obejmujących aktualizację, konfigurację MDM/MAM, oraz weryfikację aplikacji.	Z
3.21	Przeprowadzanie wideorozpraw i spotkań online wyłącznie z wykorzystaniem szyfrowanych platform, po wcześniejszym przetestowaniu E2EE, weryfikacji uczestników i zabezpieczeniu otoczenia (tło, nagrywanie, osoby w pomieszczeniu).	Z
3.22	Zakaz logowania do poczty, systemów kancelarii lub repozytoriów danych bez aktywnego połączenia VPN.	Z
3.23	Korzystanie wyłącznie z prywatnych hotspotów LTE/5G lub bezpiecznych sieci prywatnych zamiast publicznego Wi-Fi.	Z

4. Serwery i urządzenia NAS

Numer Zalecenia	Czynnik \ Adresat	1 os.
4.1	Stosowanie silnych haseł dostępowych.	Z

4.2	Stosowanie jednego hasła do kilku kont dostępnych.	N
4.3	Przeprowadzanie okresowej zmiany haseł lub stosowanie menadżera haseł.	Z
4.4	Stosowanie uwierzytelniania wieloskładnikowego (MFA).	Z
4.5	Stosowanie szyfrowania danych i komunikacji.	Z
4.6	Stosowanie darmowego oprogramowania antywirusowego przeznaczonego do użytku osobistego.	N
4.7	Stosowanie oprogramowania antywirusowego w standardzie biznesowym z rozbudowanymi modułami zapory sieciowej i ochroną korespondencji e-mail.	Z
4.8	Wykonywanie okresowych kopii zapasowych systemu operacyjnego i danych.	Z
4.9	Zapewnienie redundancji łączy i narzędzi sieciowych.	Z

5. Komunikacja w sieci Internet / sieć

Numer Zalecenia	Czynnik \ Adresat	1 os.
5.1	Stosowanie szyfrowania danych i komunikacji.	Z
5.2	Korzystanie z publicznej (w tym udostępnianej przez osoby trzecie) sieci wi-fi bez jednoczesnego korzystania z zaufanego połączenia VPN.	N
5.3	Korzystanie z prywatnej (udostępnianej przez inne podmioty, w tym klientów) sieci wi-fi bez jednoczesnego korzystania z zaufanego połączenia VPN.	N
5.4	korzystanie w miejscach publicznych z sieci udostępnianej samodzielnie od operatora telekomunikacyjnego (np. korzystając z funkcji hotspot w telefonie).	Z
5.5	Stosowanie biurowej sieci wi-fi o standardzie szyfrowania komunikacji WPA3.	Z

5.6	Korzystanie wyłącznie z odpowiednio zabezpieczonych przeglądarek internetowych.	Z
5.7	Łączenie się z zasobami Kancelarii (serwer, chmura) z sieci zewnętrznej (w tym z domowej sieci Wi-Fi) bez użycia szyfrowanego połączenia VPN.	N
5.8	Zabezpieczenie domowej sieci Wi-Fi, wykorzystywanej do celów zawodowych, zgodnie z dobrymi praktykami (m.in. silne hasło, standard szyfrowania WPA3).	Z
5.9	Korzystanie z urządzeń sieciowych (routerów, modemów, punktów dostępowych) wyłącznie po zmianie ich domyślnej konfiguracji fabrycznej, w szczególności haseł i loginów administracyjnych.	Z

6. Poczta elektroniczna

Numer Zalecenia	Czynnik \ Adresat	1 os.
6.1	Stosowanie silnych haseł dostępowych.	Z
6.2	Stosowanie jednego hasła do kilku kont dostępowych.	N
6.3	Przeprowadzanie okresowej zmiany haseł lub stosowanie menadżera haseł.	Z
6.4	Stosowanie uwierzytelniania wieloskładnikowego (MFA).	Z
6.5	Stosowanie szyfrowania wiadomości e-mail w przypadku braku szyfrowania komunikacji pomiędzy Klientami pocztowymi.	Z
6.6	Stosowanie szyfrowania lub hasłowania załączników wiadomości e-mail.	Z
6.7	W przypadku korzystania z aplikacji lub usług, w ramach których dostawcy uzyskują dostęp do danych osobowych przetwarzanych przez Kancelarię, zawarcie stosownej DPA, zgodnej z przepisami RODO i zasadami dostępu do Tajemnicy zawodowej.	Z
6.8	Korzystanie z własnego serwera pocztowego.	N
6.9	W przypadku korzystania z poczty elektronicznej w ramach Usług Online, korzystanie w modelu biznesowym wraz z zawarciem DPA.	Z

6.10	Korzystanie z darmowych skrzynek pocztowych, w tym przeznaczonych do innych niż biznesowych celów.	N
6.11	Korzystanie z rozwiązań i usług tylko zweryfikowanych zaufanych dostawców, posiadających siedzibę na terytorium EOG, którzy umożliwiają (gdy dochodzi do powierzenia przetwarzania danych osobowych) zawarcie stosownej DPA, a także przetwarzających powierzone dane na terytorium EOG.	Z
6.12	Przechowywanie (retencja) danych na terytorium EOG.	Z

7. Back-up

Numer Zalecenia	Czynnik \ Adresat	1 os.
7.1	Stosowanie silnych haseł dostępowych.	Z
7.2	Stosowanie jednego hasła do kilku kont dostępowych.	N
7.3	Przeprowadzanie okresowej zmiany haseł lub stosowanie menadżera haseł.	Z
7.4	Stosowanie uwierzytelniania wieloskładnikowego (MFA).	Z
7.5	Szyfrowanie kopii zapasowej danych.	Z
7.6	Wykonywanie dodatkowej lokalnej kopii zapasowej danych.	Z
7.7	Wykonanie kopii zapasowej systemu operacyjnego i danych przed aktualizacją oprogramowania.	Z
7.8	Stosowanie kasowania kryptograficznego dla dysków.	Z
7.9	Stosowanie niszczonek typu P-5.	Z

8. Przetwarzanie danych w Usługach Online

Numer Zalecenia	Czynnik \ Adresat	1 os.
8.1	Stosowanie silnych haseł dostępowych.	Z
8.2	Stosowanie jednego hasła do kilku kont dostępowych.	N
8.3	Przeprowadzanie okresowej zmiany haseł lub stosowanie menadżera haseł.	Z

8.4	Stosowanie uwierzytelniania wieloskładnikowego (MFA). Rozważenie wprowadzenia kluczy sprzętowych do uwierzytelniania w usługach online lub aplikacji uwierzytelniających.	Z
8.5	W przypadku korzystania z Usług Online, wybór tych Usług Online, których dostawca zapewnia szyfrowanie komunikacji i danych.	Z
8.6	Stosowanie dodatkowego (własnego) szyfrowania danych przetwarzanych w ramach Usług Chmurowych.	Z
8.7	Szyfrowanie danych przekazywanych w ramach komunikacji z zastosowaniem szyfrowania end-to-end	
8.8	W przypadku korzystania z aplikacji lub usług, w ramach których dostawcy uzyskają dostęp do danych osobowych przetwarzanych przez Kancelarię, zawarcie stosownej DPA, zgodnej z przepisami RODO i zasadami dostępu do Tajemnicy zawodowej.	Z
8.9	Korzystanie z rozwiązań i usług tylko zaufanych dostawców, posiadających siedzibę na terytorium EOG, którzy umożliwiają (gdy dochodzi do powierzenia przetwarzania danych osobowych) zawarcie stosownej DPA, a także przetwarzających powierzone dane na terytorium EOG.	Z
8.10	Korzystanie z Usług Online zapewniających możliwość kontroli logów i dostępu.	Z
8.11	Korzystanie z Usług Online wyłącznie w standardzie biznesowym.	Z
8.12	Przechowywanie (retencja) danych na terytorium EOG.	Z
8.13	Korzystanie z usług zapewniających Data Ownership Verification, zwłaszcza w usługach bazujących na przetwarzaniu danych przez LLM.	Z

9. Przekazywanie danych poza Kancelarię, w tym do klienta

Numer Zalecenia	Czynnik \ Adresat	1 os.
9.1	Stosowanie silnych haseł dostępowych.	Z
9.2	Stosowanie szyfrowania danych.	Z
9.3	Przekazywanie danych poza Kancelarię przy wykorzystaniu Usług Chmurowych w standardzie biznesowym.	Z

9.4	Przekazywanie danych poza Kancelarię przy wykorzystaniu narzędzi lub usług darmowych, w tym niezapewniających standardów biznesowych i standardów ochrony danych osobowych (np. bez DPA).	N
9.5	Przekazywanie danych poza Kancelarię na nośnikach danych bez hasła dostępu.	N
9.6	Przekazywanie zaszyfrowanych danych i hasła dostępowego przy wykorzystaniu różnych metod komunikacji.	Z

10. Biura serwisowane

Numer Zalecenia	Czynnik \ Adresat	1 os.
10.1	Stosowanie szyfrowania danych i komunikacji w przypadku wykorzystywania sieci teleinformatycznej dostarczanej w ramach usługi biura serwisowanego.	Z
10.2	Zawarcie DPA w przypadku korzystania z usług obsługi korespondencji (np. rejestracji poczty przychodzącej, skanowania poczty przychodzącej, przesyłania skanu poczty przychodzącej).	Z
10.3	Korzystanie z ogólnodostępnej sieci wi-fi zapewnianej przez administratora biura lub wynajmującego.	N
10.4	Korzystanie z ogólnodostępnego sprzętu komputerowego.	N
10.5	Korzystanie z ogólnodostępnego serwera.	N
10.6	Skanowanie lub drukowanie na sprzęcie ogólnodostępnym.	N

11. Komunikatory

Numer Zalecenia	Czynnik \ Adresat	1 os.
11.1	Stosowanie silnych haseł dostępowych.	Z
11.2	Stosowanie jednego hasła do kilku kont dostępowych.	N

11.3	Przeprowadzanie okresowej zmiany haseł lub stosowanie menadżera haseł.	Z
11.4	Stosowanie uwierzytelniania wieloskładnikowego (MFA).	Z
11.5	Korzystanie z komunikatorów niezapewniających szyfrowania danych i komunikacji typu end-to-end.	N
11.6	Korzystanie z rozwiązań i usług tylko zaufanych dostawców, posiadających siedzibę na terytorium EOG, którzy umożliwiają (gdy dochodzi do powierzenia przetwarzania danych osobowych) zawarcie stosownej DPA, a także przetwarzających powierzone dane na terytorium EOG.	Z

12. Obsługa zewnętrzna IT

Numer Zalecenia	Czynnik \ Adresat	1 os.
12.1	Korzystanie z usług zewnętrznego wsparcia informatycznego wyłącznie przy zachowaniu zasad bezpieczeństwa, w tym poufności danych znajdujących się w posiadaniu Kancelarii.	Z
12.2	Powierzenie funkcji Administratora Systemów Informatycznych zewnętrznemu dostawcy usług.	Z
12.3	Zawarcie DPA.	Z
12.4	Wsparcie lokalne w biurze Kancelarii.	Z
12.5	Wsparcie z dostępem zdalnym bez stałej kontroli dostępu przez członka Personelu Kancelarii.	N

13. Reagowanie na incydenty

Numer Zalecenia	Czynnik \ Adresat	1 os.
13.1	Okresowe testowanie kompletności i integralności posiadanych kopii zapasowych systemu operacyjnego i danych.	Z
13.2	Przygotowanie planu reagowania na Incydenty w formie checklisty.	ZO
13.3	Monitorowanie oraz rejestrowanie nietypowych i podejrzanych zdarzeń.	Z

13.4	Okresowe weryfikowanie możliwości wycieku używanych danych autoryzacyjnych przy pomocy publicznie dostępnych portali.	Z
13.5	Zgłoszenie wystąpienia Incydentu odpowiednim organom nadzorczym, klientom i innym zainteresowanym podmiotom w zakresie przewidzianym przepisami.	Z
13.6	Wykonanie analizy Incydentu po jego wystąpieniu, w celu wyciągnięcia wniosków, przeglądu zabezpieczeń i aktualizacji wdrożonych procedur bezpieczeństwa.	Z
13.7	Przywrócenie normalnego działania Kancelarii po wystąpieniu Incydentu bez przeglądu i aktualizacji zabezpieczeń i wdrożonych procedur.	N
13.8	W razie wystąpienia Incydentu, zlecenie wykonania analizy powłamaniowej zewnętrznym ekspertom, posiadającym siedzibę na terytorium EOG, którzy umożliwiają (gdy dochodzi do powierzenia przetwarzania danych osobowych) zawarcie stosownej DPA, a także przetwarzającym powierzone dane na terytorium EOG.	Z

14. Praca Zdalna i Mobilna

Numer Zalecenia	Czynnik \ Adresat	1 os.
14.1	Aktywny VPN jako warunek zdalnego dostępu do skrzynek pocztowych, repozytoriów i systemów kancelarii.	Z
14.2	Logowanie do poczty/systemów bez aktywnego VPN (w jakiegokolwiek sieci).	N
14.3	PA3-Personal (AES), unikalne silne hasło, wyłączony WPS, wyłączone zdalne zarządzanie, zmienione domyślne dane administratora.	Z
14.4	Oddzielna sieć dla urządzeń innych niż służbowe (goście, prywatne, IoT).	Z
14.5	Współdzielenie SSID urządzeń służbowych i IoT.	N
14.6	MDM/MAM na smartfonach służbowych (profil służbowy, zdalne kasowanie, polityki haseł/biometrii, wymuszanie szyfrowania, blokady kopii bez szyfrowania).	ZO
14.7	Komunikatory z E2EE do komunikacji wewnętrznej oraz z klientami krytycznymi.	Z
14.8	Szyfrowanie <i>at rest</i> i <i>in transit</i> : pełne szyfrowanie dysku	Z

	(BitLocker/FileVault/ekwiwalent), TLS dla usług, E2EE gdzie możliwe (wideo/komunikatory).	
14.9	Endpoint security klasy biznesowej (AV/EDR + zapora), aktualizacje automatyczne, definiowanie harmonogramu skanów, blokada uruchamiania nieznanych aplikacji.	Z
14.10	Polityka blokady ekranu: automatyczna blokada po krótkiej bezczynności, hasło/PIN/biometria.	Z
14.11	Polityka prywatność: korzystanie nakładek pomagających utrzymać prywatność przy pracy mobilnej; unika pracy w miejscach publicznych.	ZO
14.12	Kopie zapasowe: automatyczne, szyfrowane, testowanie przywracanie raz na kwartał; dodatkowa kopia offline / odłączana.	Z
14.13	Płatności i dostęp do repozytoriów poufnych wyłącznie przez prywatną sieć domową lub przez VPN (nigdy przez publiczne Wi-Fi).	Z
14.14	Preferencja własnego hotspotu LTE/5G zamiast publicznego WI-Fi, gry pracujesz poza domem.	Z
14.15	Korzystanie z zewnętrznych, niezauważalnych serwisów IT z dostępem zdalnym bez nadzoru.	N
14.16	Rejestr urządzeń (komputer, smartfon) z przypisaniem do użytkownika; tylko urządzenia służbowe do pracy.	Z
14.17	Korzystanie z ogólnodostępnych urządzeń do drukowania.	N
14.18	Korzystanie z urządzeń w biurze oraz z urządzeń domowych tylko w odseparowanej sieci i po akceptacji bezpieczeństwa.	Z
14.19	Korzystanie z przeglądarki i klienta poczty: wersje aktualne, zabezpieczone konfiguracje, filtrowanie phishingu/załączników, DLP (o ile możliwe).	Z

ROZDZIAŁ II. ZALECENIA DODATKOWE

dedykowane dla Kancelarii małych, średnich i dużych

Poniższe zalecenia są uzupełniające w stosunku do zaleceń Rozdziału I dla Kancelarii małych, średnich i dużych. Zalecenia z Rozdziału I i II mają zastosowanie łącznie tylko do Kancelarii małych, średnich i dużych i stanowią minimalne zabezpieczenia przetwarzania

informacji. Zalecenia Rozdziału I stosuje się wprost, chyba że w Rozdziale II przewidziano inne zalecenia.

15. Zalecenia ogólne

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
15.1	Stosowanie polityki zarządzania konfiguracją, dostępem oraz monitorowaniem aktywności w systemach i sieciach, obejmującej: (a) zasadę minimalnych uprawnień i <i>zero trust</i> ; (b) cykliczny przegląd uprawnień użytkowników (co najmniej raz na 6 miesięcy); (c) rejestrowanie i monitorowanie logów dostępu do systemów i sieci.	Z	Z	Z
15.2	Wdrożenie i utrzymywanie systemu zarządzania bezpieczeństwem informacji zgodnego z normami z rodziny ISO/IEC 27000 (w szczególności ISO/IEC 27001:2022 i 27002:2022) lub równoważnymi standardami (np. NIST CSF 2.0), z uwzględnieniem okresowych przeglądów zgodności (audytów wewnętrznych).	ZO	Z	Z
15.3	Wdrożenie i okresowe aktualizowanie (nie rzadziej niż raz w roku) wewnętrznych polityk bezpieczeństwa obejmujących: (a) ochronę danych i tajemnicy zawodowej; (b) zarządzanie dostępem i rolami; (c) zasady klasyfikacji i retencji informacji; (d) pracę zdalną i mobilną; (e) zasady korzystania z narzędzi opartych na sztucznej inteligencji. Stosowanie zasady <i>zero trust</i> w dostępie do informacji oraz nadawanie dostępu wyłącznie w zakresie niezbędnym do realizacji zadań (<i>need to know</i>), tj. nadawanie dostępu na zasadzie minimalnych uprawnień, z wykorzystaniem wieloskładnikowego uwierzytelniania (MFA). Systemy informatyczne i repozytoria dokumentów powinny umożliwiać nadawanie uprawnień per osoba lub zespół. Przy zakończeniu współpracy – natychmiastowe odebranie dostępu (<i>offboarding T-O</i>) oraz weryfikacja zwrotu sprzętu i nośników danych. Przy zakończeniu współpracy uprawnienia winny zostać trwale na stałe. Wdrożenie formalnej polityki klasyfikacji informacji, obejmującej etykietowanie spraw według poziomu poufności (np. publiczna / wewnętrzna / tajemnica adwokacka), zasady	ZO	Z	Z

	czyszczenia metadanych z dokumentów (DOCX, PDF, EXIF) przed ich wysyłką oraz politykę retencji i niszczenia danych (również w kontekście obowiązków <i>litigation hold</i>).			
15.4	Wdrożenie i testowanie (co najmniej raz w roku) planu ciągłości działania (BCP) oraz planu reagowania na incydenty i odzyskiwania danych (IRP/DRP), obejmujących: (a) zasady kopii zapasowych, (b) procedury komunikacji kryzysowej, (c) przydział ról i odpowiedzialności w razie incydentu.	ZO	Z	Z
15.5	Prowadzenie obowiązkowych szkoleń wstępnych oraz cyklicznych (nie rzadziej niż raz w roku) z zakresu bezpieczeństwa informacji, ochrony danych osobowych, reagowania na incydenty oraz bezpiecznego korzystania z technologii (w tym AI). Szkolenia powinny być dokumentowane i oceniane.	Z	Z	Z
15.6	Powierzenie administrowania i nadzoru nad infrastrukturą informatyczną osobie lub podmiotowi pełniącemu funkcję Administratora Systemu Informatycznego (ASI), z obowiązkiem: (a) prowadzenia rejestru incydentów i zmian; (b) niezwłocznego zgłaszania naruszeń ochrony danych; (c) okresowego raportowania o stanie bezpieczeństwa.	ZO	Z	Z
15.7	Posiadanie aktualnego ubezpieczenia obejmującego ryzyka cybernetyczne i naruszenia ochrony danych osobowych, w tym: (a) koszty przywrócenia działania systemów, (b) obsługę prawno-techniczną incydentu, (c) szkody klienta wynikłe z ujawnienia danych.	Z	Z	Z
15.8	Aktualizacja oprogramowania i konfiguracji systemów w sposób kontrolowany, z wykorzystaniem środowiska testowego, po uprzedniej ocenie ryzyka i zgodności z polityką bezpieczeństwa. Wdrożenie systemu zarządzania poprawkami (patch management) oraz okresowych testów podatności.	ZO	ZO	Z
15.9	Wdrożenie zasad bezpieczeństwa dostawców usług i rozwiązań IT (w tym chmurowych i AI), obejmujących audyt bezpieczeństwa przed nawiązaniem współpracy oraz coroczny przegląd zgodności z umowami powierzenia danych.	Z	Z	Z

15.10	Zakaz wprowadzania informacji objętych Tajemnicą zawodową do publicznych systemów AI lub narzędzi przetwarzanych poza kontrolą Kancelarii; dopuszczenie wyłącznie narzędzi zatwierdzonych wewnątrz i spełniających wymogi bezpieczeństwa danych.	Z	Z	Z
15.11	Organizowanie corocznych szkoleń oraz praktycznych ćwiczeń dla personelu (w tym współpracowników i praktykantów) dotyczących: reagowania na incydenty, rozpoznawania ataków socjotechnicznych i fałszywych komunikatów, postępowania z danymi objętymi tajemnicą zawodową oraz bezpiecznego korzystania z narzędzi AI i chmury.	ZO	Z	Z

16. Komputery PC i przenośne

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
16.1	Korzystanie przez Personel z prywatnego sprzętu w celach zawodowych.	N	N	N
16.2	Korzystanie przez Personel w celach zawodowych wyłącznie ze sprzętu służbowego.	Z	Z	Z
16.3	Korzystanie z zewnętrznego serwisu IT w formie zdalnej bez bieżącego nadzoru członka Personelu.	N	N	N
16.5	Wdrożenie stosowania Haseł administratora.	Z	Z	Z
16.6	Korzystanie z rozwiązań zapewniających bezpieczne uwierzytelnianie (np.: menedżera haseł lub aplikacji pozwalających na wieloskładnikową identyfikację)	Z	Z	Z

17. Smartfon

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
17.1	Korzystanie przez Personel z prywatnego sprzętu w celach zawodowych.	N	N	N
17.2	Korzystanie przez Personel w celach zawodowych	Z	Z	Z

	wyłącznie ze sprzętu służbowego.			
17.3	Prowadzenie ewidencji sprzętu powierzono Personelowi.	Z	Z	Z

18. Serwery i urządzenia NAS

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
18.1	Opracowanie i wdrożenie formalnej polityki bezpieczeństwa informacji.	Z	Z	Z
18.2	Monitoring i ślady audytowe	Z	Z	Z

19. Poczta elektroniczna

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
19.1	Korzystanie z własnego serwera pocztowego.	N	ZO	Z
19.2	Wdrożenie i stosowanie formalnej procedury (checklisty) weryfikacji bezpieczeństwa dostawców usług poczty elektronicznej i usług powiązanych.	ZO	Z	Z

20. Back-up

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
20.1	Wdrożenie polityki wydawania danych uprawnionym organom w przypadkach określonych przepisami prawa.	Z	Z	Z

21. Przetwarzanie danych w Usługach Online

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
21.1	Wdrożenie polityki wydawania danych uprawnionym organom w przypadkach określonych przepisami prawa.	Z	Z	Z

22. Przekazywanie danych poza Kancelarię, w tym do klienta

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
22.1	Wdrożenie polityki przekazywania danych w przypadkach określonych przepisami prawa.	Z	Z	Z

23. Obsługa zewnętrzna IT

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
23.1	Korzystanie z usług podmiotu posiadającego zweryfikowaną wiedzę z zakresu rozwiązań sieciowych i ISO z rodziny ISO/IEC 27000.	ZO	Z	Z

24. Reagowanie na Incydenty

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
24.1	Wdrożenie polityki zarządzania Incydentami.	Z	Z	Z
24.2	Prowadzenie rejestru Incydentów.	Z	Z	Z
24.3	Wyznaczenie zespołu reagowania na Incydenty, w tym zdefiniowanie ról i odpowiedzialności poszczególnych osób.	ZO	Z	Z
24.4	Powierzenie zadań zespołu reagowania na Incydenty w całości zewnętrznemu dostawcy.	N	N	N
24.5	Opracowanie planów komunikacji z klientami, mediami lub innymi podmiotami zainteresowanymi na wypadek wystąpienia Incydentu	ZO	Z	Z
24.6	Okresowy przegląd darknetu pod kątem potencjalnych wycieków danych lub korzystanie z usług podmiotu świadczącego tego typu usługi.	ZO	ZO	ZO
24.7	Okresowe przeprowadzanie szkoleń obejmujących ćwiczenia z wystąpienia Incydentu.	ZO	ZO	ZO

25. Praca zdalna i mobilna

Numer	Czynnik \ Adresat	małe	średnie	duże
-------	-------------------	------	---------	------

Zalecenia				
25.1	Polityka pracy zdalnej (zakres dozwolonych lokalizacji, wymagania dot. łączy, urządzeń, VPN, E2EE, białe listy narzędzi, zasada najmniejszych uprawnień).	Z	Z	Z
25.2	Białe listy komunikatorów z E2EE oraz wideokonferencji (lista dozwolona/zakazana; okresowy przegląd).	ZO	Z	Z
25.3	Zakaz logowania bez aktywnego VPN (monitoring wymuszenia po stronie serwera).	ZO	Z	Z
25.4	Kwartalny self-check bezpieczeństwa stanowiska pracy zdalnej.	ZO	Z	Z
25.5	Bezpieczne przygotowanie stanowiska wideorozprawy/spotkania – checklista.	Z	Z	Z
25.6	MDM/MAM: wymuszenie polityk (PIN/biometria, szyfrowanie, blokady debugowania, zdalne wipe, separacja danych służbowych).	ZO	Z	Z
25.7	Wprowadzenie polityki BYOD: dozwolone wyłącznie z MDM/MAM; BYOD bez MDM – zakazane.	Z	Z	Z
25.8	Rejestr urządzeń i dostępu (audyt logów, inspekcja konfiguracji; odwołanie uprawnień po utracie/zmianie).	Z	Z	Z
25.9	Procedura incydentowa specyficzna dla pracy zdalnej (zgłoszenie, odcięcie dostępu, wymuszone resetowanie poświadczeń, forensyka).	ZO	Z	Z
25.10	Szkolenia ukierunkowane na zdalne zagrożenia (phishing, vishing, deepfake w wideorozprawach, bezpieczeństwo fizyczne w domu).	Z	Z	Z
25.11	Kontrola nośników i druku: szyfrowane nośniki; zakaz przenoszenia danych na niezabezpieczone pendrive'y; polityka „czystego biurka”.	Z	Z	Z
25.12	Przy użyciu VPN - wprowadzenie blokady po stronie serwera dla logowań spoza VPN.	Z	Z	Z
25.13	Współpraca z IT: wsparcie lokalne/zdalne pod nadzorem; umowa o poufności; brak dostępu zdalnego ad-hoc bez autoryzacji.	Z	Z	Z

Załącznik numer 1 do Dobrych Praktyk dotyczących cyberbezpieczeństwa w działalności kancelarii adwokackich i pracy Adwokata

Niniejszy załącznik do *Dobrych Praktyk* stanowi opis zaleceń określonych w głównej części:

ROZDZIAŁ I. ZALECENIA PODSTAWOWE

dedykowane dla Kancelarii jednoosobowych, bazowe dla pozostałych grup Kancelarii

NUMER ZALECENIA	CZEGO DOTYCZY?	WYJAŚNIENIA
1.1 14.7 14.9 14.19	Korzystanie wyłącznie z licencjonowanego i aktualnego oprogramowania przeznaczonego do komercyjnego zastosowania.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ korzystanie z oprogramowania na podstawie licencji do użytku komercyjnego, uzyskanej od podmiotu uprawnionego i zgodnie z jej warunkami, ➤ przeprowadzanie regularnych aktualizacji systemu operacyjnego i pozostałego oprogramowania / aplikacji wykorzystywanych na serwerach, komputerach i urządzeniach mobilnych oraz pozostałym sprzęcie (<i>firmware</i>, np. na routerach), ➤ instalowanie aktualizacji oprogramowania bez zbędnej zwłoki, w szczególności w przypadku łat bezpieczeństwa udostępnionych w związku z wykryciem luk, ➤ stosowanie aktualizacji automatycznych lub wykorzystujących aktualizacje wymagające ustalenia z użytkownikiem czasu przeprowadzenia aktualizacji, ➤ korzystanie z komunikatorów E2EE, ➤ endpoint security klasy biznesowej, ➤ korzystanie z narzędzi z “białej listy” kancelarii / operatora IT.

		<p><u>Niezalecane jest:</u></p> <p>korzystanie w celach zawodowych z oprogramowania przeznaczonego wyłącznie do użytku osobistego lub edukacyjnego (np. freeware, shareware),</p> <ul style="list-style-type: none"> ➤ korzystanie w celach zawodowych ze sprzętu komputerowego wyposażonego w system operacyjny Windows w wersji innej niż PRO lub Enterprise, ➤ korzystanie z nieautoryzowanych przez producenta oprogramowania modyfikacji oprogramowania (w szczególności w przypadku systemu operacyjnego przeznaczonego dla telefonów komórkowych typu smartphone), ➤ instalowanie aplikacji mobilnych pobranych spoza autoryzowanych sklepów aplikacji (m.in. Google Store, Apple Store) lub ze źródeł nie pochodzących od producenta, ➤ korzystanie z oprogramowania względem którego producent nie zapewnia wsparcia i aktualizacji.
<p>2.1 3.1 4.1 6.1 7.1 8.1 9.1 11.1 14.3 14.6 14.10 25.4</p>	<p>Stosowanie silnych haseł dostępowych.</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ w celu zachowania kontroli dostępu i ochrony przed kompromitacją (przełamaniem) haseł słabych – stosowanie silnych haseł dostępowych do logowania we wszelkich punktach dostępowych (np. kont użytkownika, sprzęcie, aplikacjach itp.), ➤ w przypadku, gdy jest to technicznie możliwe (np. hasło/pin nie jest ograniczony tylko do 4-6 znaków, np. w telefonie komórkowym) – stosowanie haseł złożonych co najmniej z 12 znaków diaktrycznych (w tym duża i mała litera, cyfra lub znak specjalny), ➤ w przypadku dostępów w rzadko wykorzystywanych aplikacjach lub portalach – stosowanie jednorazowego losowo wybranego hasła (kolejne logowanie może nastąpić przy wykorzystaniu funkcji przypomnienia hasła), ➤ stosowanie hasła dostępowego na komputerach na poziomie BIOS, korzystanie (o ile jest to

		<p>możliwe) z automatycznego blokowania dostępu w przypadku niepoprawnego podania hasła (np. po 3 nieudanej próbie logowania),</p> <ul style="list-style-type: none"> ➤ w przypadku bezczynności użytkownika (o ile jest to możliwe) – stosowanie automatycznego wylogowania z konta/usługi, ➤ zmiana haseł krytycznych co kwartał. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ aby hasło bazowało na łatwo identyfikowalnych powiązaniach z osobą użytkownika, organizacją lub usługą, do której jest to dostęp, ➤ udostępnianie innym osobom (w tym współpracownikom lub rodzinie) hasła do konta przypisanego do określonego użytkownika.
2.2 3.2 4.2 6.2 7.2 8.2 11.2	Stosowanie jednego hasła do kilku kont dostępowych.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ w przypadku korzystania z większej ilości haseł – korzystanie z menadżera haseł lub sprzętowych tokenów U2F. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ stosowanie jednego hasła do kilku kont dostępowych; zwiększa to ryzyko kompromitacji hasła i w konsekwencji wycieku danych poufnych, w tym objętych Tajemnicą zawodową.
2.3 3.3 4.3 6.3 7.3 8.3 11.3 25.4	Przeprowadzanie okresowej zmiany haseł lub stosowanie menadżera haseł.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ stosowanie menadżera haseł lub przeprowadzanie okresowej zmiany haseł, przy czym decyzja w tym przedmiocie powinna uwzględniać przyjętą w Kancelarii klasyfikację przetwarzanych informacji oraz wdrożone procedury. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ przeprowadzanie zbyt częstej zmiany haseł (np. co kilka dni); skutkować to może utratą dostępu lub kompromitacją stosowanych haseł.
2.4	Stosowanie	Uwierzytelnianie wieloskładnikowe (MFA) zwiększa

<p>3.4 4.4 6.4 7.4 8.4 11.4</p>	<p>uwierzytelniania wieloskładnikowego (MFA).</p>	<p>poziom bezpieczeństwa procesu logowania i dostępu do danych przetwarzanych w zasobach, do których użytkownik podjął próbę logowania. W przypadku kompromitacji hasła, logowanie nie jest możliwe bez dodatkowej autoryzacji.</p> <p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ w przypadku, gdy jest to technicznie możliwe i dostępne – stosowanie uwierzytelniania wieloskładnikowego (MFA), ➤ korzystanie z dostępnych aplikacji MFA. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ wykorzystywanie w procesie wieloskładnikowego uwierzytelniania (poza hasłem) jedynie haseł/kodów dostępu przesyłanych w treści wiadomości tekstowych na numery telefonu komórkowego.
<p>2.5 3.5 4.5 5.1 5.5 6.5 6.6 7.5 8.5 8.6 9.2 10.1 11.5 14.1 14.2 14.8 14.12 25.4</p>	<p>Stosowanie szyfrowania danych i komunikacji.</p> <p>Stosowanie szyfrowania wiadomości e- mail w przypadku braku szyfrowania komunikacji pomiędzy Klientami pocztowymi (programami pocztowymi).</p> <p>Stosowanie szyfrowania lub hasłowania załączników wiadomości e-mail.</p> <p>Szyfrowanie kopii zapasowej danych.</p> <p>W przypadku korzystania z Usług Online wybór tych Usług Online, których dostawca zapewnia szyfrowanie komunikacji i danych.</p> <p>Stosowanie</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ korzystanie z komputerów wykorzystujących procesory wyposażone w moduł TPM lub spełniające podobne funkcje, ➤ w przypadku korzystania z komputerów wyposażonych w system operacyjny Windows oraz procesory z modułem TPM – aktywowanie funkcjonalności BitLocker, służącej do szyfrowania dysku (w przypadku sprzętu z systemem operacyjnym macOS zalecane jest aktywowanie funkcjonalności FileVault), ➤ szyfrowanie danych znajdujących się w posiadaniu Kancelarii (w szczególności objętych Tajemnicą zawodową obrońcą), ➤ szyfrowanie z poziomu ustawień BIOS wraz z hasłem dostępowym na poziomie BIOS, ➤ szyfrowanie danych objętych Tajemnicą zawodową przy wykorzystaniu co najmniej algorytmu AES 128 bit z kluczem 256 bitowym, ➤ stosowanie (o ile jest to możliwe) szyfrowania komunikacji end-to-end, a w przypadku braku

	<p>dodatkowego (własnego) szyfrowania danych przetwarzanych w ramach Usługi Chmurowej.</p> <p>Stosowanie szyfrowania danych i komunikacji w przypadku wykorzystywania sieci dostarczanej w ramach usługi biura serwisowanego.</p> <p>Korzystanie z komunikatorów niezapewniających szyfrowania danych i komunikacji typu <i>end-to-end</i>.</p>	<p>możliwości stosowania tej metody, zaleca się stosowanie Szyfrowania <i>in transit</i> (wraz z Szyfrowaniem <i>at rest</i> przechowywanych danych),</p> <ul style="list-style-type: none"> ➤ szyfrowanie kopii zapasowych (back-up) danych, ➤ szyfrowanie całej wiadomości e-mail w przypadku braku szyfrowania komunikacji pomiędzy Klientami pocztowymi, ➤ szyfrowanie lub hasłowanie załączników do wiadomości e-mail, ➤ w przypadku korzystania z Usług Online, wybór tych Usług Online, których dostawca zapewnia szyfrowanie komunikacji i danych, z zastrzeżeniem że mimo korzystania z Usług Chmurowych, których dostawca zapewnia takie szyfrowanie, zalecane jest dodatkowe własne szyfrowanie danych przekazywanych i przechowywanych w Usłudze Chmurowej (w celu uniemożliwienia dostawcy zapoznania się z treścią danych), ➤ w przypadku wykorzystywania sieci teleinformatycznej dostarczanej w ramach usługi biura serwisowanego – szyfrowanie danych i komunikacji prowadzonej przy wykorzystaniu tej sieci (w szczególności stosowanie szyfrowania transmisji danych przy pomocy VPN lub routerów obsługujących protokoły szyfrujące i umożliwiających ich aktywne wykorzystanie (w standardzie WPA3), ➤ w przypadku korzystania z narzędzi służących do wideokonferencji zaleca się stosowanie tych zapewniających szyfrowanie komunikacji end-to-end lub przynajmniej stosujących Szyfrowanie <i>in transit</i>. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ korzystanie z komunikatorów niezapewniających szyfrowania danych i komunikacji typu end-to-end, ➤ przekazywanie odbiorcom (w tym klientom) niezabezpieczonych szyfrowaniem lub hasłem danych objętych Tajemnicą zawodową).
--	---	---

<p>2.6 2.7 3.6 3.7 4.6 4.7</p>	<p>Stosowanie darmowego oprogramowania antywirusowego przeznaczonego do użytku osobistego.</p> <p>Stosowanie oprogramowania antywirusowego w standardzie biznesowym z rozbudowanymi modułami zapory sieciowej i ochroną korespondencji e-mail.</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ stosowanie odpowiedniego oprogramowania antywirusowego (na każdym sprzęcie, a nie tylko komputerach) w standardzie biznesowym, tj. dedykowanego do zastosowania przez co najmniej mikro przedsiębiorców (w celach komercyjnych), ➤ stosowanie oprogramowania antywirusowego rozbudowanego o moduły zapory sieciowej oraz moduł filtrowania korespondencji e-mail (np. w zakresie ochrony antyphishingowej). <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ stosowanie darmowego oprogramowania antywirusowego z uwagi na niski poziom ochrony dostarczanej przez takie oprogramowanie (m.in. w związku z ograniczonymi funkcjonalnościami oraz rzadko aktualizowanymi bazami sygnatur wirusów).
<p>2.8 3.8 3.9 4.8 7.6 7.7 7.8 7.9 13.1</p>	<p>Wykonywanie okresowych kopii zapasowych systemu operacyjnego i danych.</p> <p>Wykonywanie okresowych kopii zapasowych danych na urządzeniu zewnętrznym.</p> <p>Wykonywanie okresowych kopii zapasowych danych objętych Tajemnicą zawodową w Usługach Online producenta sprzętu lub operatora telekomunikacyjnego.</p> <p>Wykonywanie dodatkowej lokalnej kopii zapasowej danych.</p> <p>Wykonanie kopii zapasowej systemu</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ wykonywanie kopii zapasowych systemu operacyjnego zainstalowanego na komputerach i serwerach przed każdą jego aktualizacją, ale nie rzadziej niż raz na kwartał, ➤ wykonywanie okresowych kopii zapasowych danych i aplikacji z telefonu komórkowego nie rzadziej niż raz na miesiąc, ➤ wykonywanie okresowych kopii zapasowych danych przechowywanych na sprzęcie komputerowym i serwerach, w tym korespondencji e-mail i wytworzonych dokumentów, raz dziennie, ale nie rzadziej niż raz na tydzień, ➤ o ile to możliwe technicznie i z uwagi na przyjęte zasady bezpieczeństwa – wykonywanie kopii zapasowych w sposób automatyczny, ➤ oprócz szyfrowania kopii zapasowych – monitorowanie dostępu do kopii zapasowych oraz ich zabezpieczenie hasłem dostępu,

	<p>operacyjnego i danych przed aktualizacją oprogramowania.</p> <p>Stosowanie kasowania kryptograficznego dla dysku.</p> <p>Stosowanie niszczonek typu P-5.</p> <p>Okresowe testowanie kompletności i integralności posiadanych kopii zapasowych systemu operacyjnego i danych.</p>	<ul style="list-style-type: none"> ➤ w przypadku wykonywania kopii zapasowych na zewnętrznym nośniku danych – wykonywanie kopii zapasowych na dyskach zewnętrznych HDD zabezpieczonych przed dostępem osób nieuprawnionych, ➤ kasowanie kryptograficzne ma na celu bezpieczne usunięcie lub zniszczenie klucza szyfrującego używanego przez dysk. Brak klucza powoduje, że dane są nie do odzyskania. Jest to szybka i bezpieczna metoda usuwania danych, ➤ stosowanie niszczonek typu P-5 zapewnia wysoki poziom bezpieczeństwa przy niszczeniu dokumentów, ➤ Okresowe testowanie kompletności i integralności posiadanych kopii zapasowych, poprzez weryfikację możliwości odzyskania danych po wystąpieniu Incydentu. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ korzystanie z funkcjonalności dostarczanych przez producenta sprzętu lub operatora telekomunikacyjnego pozwalających na wykonanie kopii zapasowej (back-up) danych objętych Tajemnicą zawodową w Usługach Online bez DPA, ➤ wykonywanie kopii zapasowych wyłącznie w Usługach Online, w szczególności w Usłudze Chmurowej z włączoną funkcjonalnością automatycznej synchronizacji wersji plików (w przypadku usunięcia lub zmiany danych lokalnie dojdzie do zmiany/usunięcia danych przechowywanych w Usłudze Chmurowej), ➤ przechowywania kopii zapasowych w ramach jednego serwera, na tym samym dysku lub dyskach zamontowanych w tym samym serwerze lub komputerze (kopie zapasowe powinny być przechowywane w środowisku odrębnym od środowiska wykorzystywanego do codziennej pracy), ➤ wykonywanie kopii zapasowych na pendrive'ach (pamięć USB) lub nośnikach
--	---	---

		wykorzystujących pamięć typu flash (np. dyski SSD).
2.9 2.10 2.11 2.12 2.13 2.14 2.15 2.16 3.10 3.11 3.12 3.13 3.14 4.9	<p>Utrzymanie stałej kontroli nad wykorzystywanym sprzętem.</p> <p>Stosowanie wygaszacza ekranu.</p> <p>Korzystanie z oprogramowania umożliwiającego zdalne zablokowanie dostępu lub usunięcie danych ze sprzętu w przypadku zgubienia lub kradzieży sprzętu.</p> <p>Korzystanie z prywatnego sprzętu w celach zawodowych.</p> <p>Korzystanie w celach zawodowych wyłącznie ze sprzętu służbowego.</p> <p>Udostępnianie sprzętu służbowego osobie trzeciej (w tym członkowi rodziny) do korzystania.</p> <p>Korzystanie z zewnętrznego serwisu IT w formie zdalnej bez bieżącego nadzoru.</p> <p>Przekazywanie sprzętu do naprawy (z danymi) bez nadzoru.</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ stosowanie środków umożliwiających utrzymanie właściwej kontroli nad sprzętem wykorzystywanym w celach zawodowych, np. hasła administratora znane jedynie Adwokatowi, zakaz wnoszenia sprzętu poza Kancelarię, itp., ➤ korzystanie z oprogramowania umożliwiającego zdalne zablokowanie dostępu lub usunięcie danych ze sprzętu w przypadku zgubienia lub kradzieży, ➤ korzystanie na komputerach z wygaszaczy ekranu i automatycznego blokowania ekranu urządzenia (w tym telefonu) po krótkiej beczynności i ponowne inicjowanie po wpisaniu hasła, ➤ w przypadku wycofania z użycia sprzętu należy zadbać o właściwe zabezpieczenie danych na nich przetwarzanych, tj. Kancelaria powinna archiwizować wycofane nośniki danych (dyski, pendrive, nośniki danych) albo zapewnić ich protokolarne zniszczenie przez specjalistyczne podmioty świadczące usługi tego typu, ➤ usuwanie zużytego sprzętu wraz z profesjonalnym zniszczeniem dysków twardej (lub ich zachowaniem przez kancelarię). <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ korzystanie z zewnętrznego serwisu IT w formie zdalnej bez bieżącego nadzoru, ➤ w przypadku awarii sprzętu – przekazywanie sprzętu do serwisu (bez usunięcia danych) bez nadzoru.
2.17 3.15	Ograniczenie lub wyłączenie działania w tle aplikacji i standardów	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ ograniczenie lub wyłączenie działania aplikacji w tle oraz standardów komunikacji, które nie są wykorzystywane w sposób stały i konieczny

	komunikacji, które nie są wykorzystywane w sposób stały i konieczny.	(w szczególności, zaleca się wyłączenie funkcji komunikacji bluetooth i wi-fi poza przypadkami świadomego korzystania z tej formy transmisji danych), ponieważ możliwe jest niezauważone ich wykorzystanie przez osobę nieuprawnioną.
6.7 8.7 10.2	<p>W przypadku korzystania z aplikacji lub usług, w ramach których dostawcy uzyskają dostęp do danych osobowych przetwarzanych przez Kancelarię, zawarcie stosownej DPA, zgodnej z przepisami RODO i zasadami dostępu do Tajemnicy zawodowej.</p> <p>Zawarcie DPA w przypadku korzystania z usług obsługi korespondencji (rejestracji poczty przychodzącej, skanowania poczty przychodzącej, przesyłania skanu poczty przychodzącej).</p> <p>Korzystanie z usług skanowania poczty przychodzącej.</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ w przypadku korzystania z aplikacji lub usług, w ramach których dostawcy uzyskują dostęp do danych osobowych przetwarzanych przez Kancelarię – zawarcie stosownej DPA, zgodnej z przepisami RODO i zasadami dostępu do Tajemnicy zawodowej (w szczególności jest to istotne w przypadku Usług Chmurowych, w tym usługi poczty elektronicznej dostarczanej w modelu Chmury Obliczeniowej), ➤ w przypadku korzystania z usług biur serwisowanych w zakresie obsługi korespondencji (rejestracji poczty przychodzącej, skanowania poczty przychodzącej, przesyłania skanu poczty przychodzącej) – zawarcie stosownej DPA. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ w przypadku korzystania z usług biur serwisowanych – korzystanie z usług skanowania poczty przychodzącej w celu uniemożliwienia zapoznania się przez pracowników biura serwisowanego z zawartością korespondencji adresowanej do Kancelarii.
5.2 5.3 5.4 5.5 5.6 10.3	<p>Korzystanie z publicznej (w tym udostępnianej przez osoby trzecie) sieci wi-fi bez jednoczesnego korzystania z zaufanego połączenia VPN.</p> <p>Korzystanie z prywatnej (udostępnianej przez zaufane podmioty, w tym klientów) sieci wi-fi bez jednoczesnego</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ korzystanie wyłącznie z bezpiecznych (co najmniej zapewniających logowanie się) połączeń internetowych i transmisji danych, ➤ jeśli korzystanie z transmisji danych jest konieczne poza biurem Kancelarii – korzystanie z sieci operatora telekomunikacyjnego, z którym Kancelaria ma zawartą umowę, lub przy wykorzystaniu zaufanych wirtualnych sieci prywatnych (tuneli VPN), ➤ w przypadku korzystania z biurowej sieci wi-fi

	<p>korzystania z zaufanego połączenia VPN.</p> <p>Jeśli jest to konieczne, korzystanie w miejscach publicznych z sieci udostępnianej samodzielnie od operatora telekomunikacyjnego (np. korzystając z funkcji hotspot w telefonie).</p> <p>Stosowanie biurowej sieci wi-fi o standardzie szyfrowania komunikacji (WPA3).</p> <p>Korzystanie wyłącznie z odpowiednio zabezpieczonych przeglądarek internetowych.</p> <p>Korzystanie z ogólnodostępnej sieci wi-fi zapewnianej przez administratora biura lub wynajmującego.</p>	<p>Kancelarii – korzystanie z sieci wi-fi o standardzie szyfrowania komunikacji WPA3,</p> <ul style="list-style-type: none"> ➤ w przypadku korzystania z narzędzi służących do wideokonferencji – stosowanie narzędzi zapewniających szyfrowanie komunikacji end-to-end lub przynajmniej stosujących Szyfrowanie <i>in transit</i>, ➤ korzystanie wyłącznie z zaufanych i odpowiednio zabezpieczonych przeglądarek internetowych, ➤ regularne aktualizowanie aplikacji przeglądarek internetowych, w tym w sposób automatyczny, ➤ korzystanie z przeglądarek po zastosowaniu wtyczek i funkcjonalności oprogramowania m.in. antywirusowego, zapory sieciowej, ➤ aby przeglądarki internetowe korzystały (o ile to technicznie możliwe i zasadne) z rozwiązań ochrony typu endpoint⁵, wtyczek blokujących okienka popup⁶, ➤ wyłączenie w ustawieniach przeglądarki internetowej funkcji autouzupełniania, ➤ aby strona internetowa Kancelarii była właściwie zabezpieczona, w tym posiadała certyfikat SSL/TLS, ➤ w przypadku korzystania na stronie internetowej Kancelarii z formularzy kontaktowych zalecane jest stosownie mechanizmu CAPTCHA oraz odpowiednie zastosowanie przepisów RODO. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ korzystanie z komunikacji internetowej pochodzącej z publicznie dostępnego wi-fi lub wi-fi znajdującego się w posiadaniu i pod nadzorem niezauważonych osób trzecich (w szczególności dotyczy do wi-fi dostępnego w biurach serwisowanych) bez jednoczesnego korzystania z zaufanego połączenia VPN, ➤ korzystanie z komunikacji internetowej pochodzącej z wi-fi znajdującego się
--	--	--

		<p>w posiadaniu i pod nadzorem osób trzecich (np. sieć klienta) bez jednoczesnego korzystania z zaufanego połączenia VPN,</p> <ul style="list-style-type: none"> ➤ korzystanie z usług kafejek internetowych w celach zawodowych, ➤ prowadzenie komunikacji z potencjalnymi klientami za pośrednictwem strony internetowej Kancelarii (chat lub formularz kontaktowy) w sprawach innych niż w celu nawiązania kontaktu z uwagi na możliwość przejęcia komunikacji przez osoby nieupoważnione.
<p>1.3 6.11 8.8 11.6 6.12 8.11 13.8</p>	<p>Korzystanie z rozwiązań i usług informatycznych tylko od zaufanych dostawców, posiadających siedzibę na terytorium EOG, którzy umożliwiają (gdy dochodzi do powierzenia przetwarzania danych osobowych) zawarcie stosownej DPA, a także przetwarzających powierzone dane na terytorium EOG.</p> <p>Przechowywanie (retencja) danych na terytorium EOG.</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ korzystanie przede wszystkim z rozwiązań i usług informatycznych od zaufanych dostawców mających siedzibę na terytorium EOG oraz przetwarzających dane Kancelarii na terytorium EOG, ➤ w przypadku powierzenia przetwarzania danych osobowych – zawarcie stosownej DPA, ➤ korzystanie z rozwiązań i usług, które są regularnie aktualizowane przez dostawcę, ➤ przed wyborem rozwiązania i usług – przeprowadzenie (w tym przy udziale zewnętrznego specjalisty, jeśli Kancelaria nie posiada odpowiednich zasobów wiedzy i umiejętności w tym zakresie) szczegółowej weryfikacji rozwiązania i usługi pod kątem zasad bezpieczeństwa informatycznego, przepisów prawa oraz wymogów związanych z przetwarzaniem Tajemnicy zawodowej; ➤ w przypadku jakichkolwiek wątpliwości odnośnie dostawcy usług lub jakości i bezpieczeństwa świadczonych usług – rezygnację z wyboru lub korzystania z danego rozwiązania lub usługi; ➤ korzystanie z rozwiązań i usług, których dostawcy umożliwiają wybór lokalizacji przechowywania danych; ➤ Zaleca się, aby przed nawiązaniem współpracy

		<p>z dostawcą usług IT, chmurowych lub komunikacyjnych, Kancelaria przeprowadziła ocenę ryzyka związanego z bezpieczeństwem usług (tzw. audyt lub checklistę bezpieczeństwa), w tym weryfikację certyfikatów (np. ISO/IEC 27001, SOC 2) oraz lokalizacji danych. Rekomendowane jest prowadzenie rejestru dostawców i coroczny przegląd ich zgodności z umowami powierzenia przetwarzania danych (DPA). Wskazane jest także monitorowanie zmian u dostawcy, takich jak wprowadzenie podprocesorów, zmiana lokalizacji danych czy incydenty bezpieczeństwa.</p> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ korzystanie z rozwiązań i usług, które nie umożliwiają przechowywania danych na terytorium EOG, <u>z zastrzeżeniem że, w przypadku konieczności wyboru miejsca przetwarzania danych poza terytorium EOG należy w pierwszej kolejności rozpatrzyć możliwość przetwarzania na terytorium EFTA lub terytorium UK (z wyłączeniem terytoriów zależnych).</u>
<p>6.8 6.9 6.10 6.12 6.13</p>	<p>Korzystanie z własnego serwera pocztowego.</p> <p>W przypadku korzystania z poczty elektronicznej w ramach Usług Online, korzystanie w modelu biznesowym wraz z zawarciem DPA.</p> <p>Korzystanie z darmowych skrzynek pocztowych, w tym przeznaczonych do innych niż zawodowych celów.</p> <p>Przechowywanie (retencja) danych na terytorium EOG.</p> <p>Przechowywanie</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ w przypadku korzystania przez Kancelarię ze skrzynek korespondencji e-mail w modelu SaaS konieczne jest wykorzystywanie w tym celu wyłącznie zaufanych Dostawców Usług Chmurowych, ➤ korzystanie z usługi poczty elektronicznej wyłącznie w standardzie biznesowym, wraz z zawarciem stosownego DPA (uwzględniającego ewentualne przetwarzanie danych szczególnych w rozumieniu RODO i Tajemnicy zawodowej), ➤ korzystanie z usług korespondencji e-mail umożliwiających przechowywanie danych na terytorium EOG, ➤ okresowa archiwizacja danych (wiadomości i załączników) poza Klientem pocztowym, ➤ prawidłowa konfiguracja narzędzi

	(retencja) danych na terytorium poza EOG.	<p>antyspamowych (wraz z właściwymi regułami) oraz stosowanie zapory sieciowej,</p> <p>W nawiązaniu również do zaleceń określonych w pkt 6.5 i 6.6:</p> <ul style="list-style-type: none"> ➤ należy dołożyć szczególnej staranności związanej z zapewnieniem poufności korespondencji przesyłanej poza Kancelarię, z zastrzeżeniem, że z uwagi na ograniczone możliwości techniczne, Kancelaria może od nich odstąpić według własnej oceny koniecznych do zastosowania środków, ➤ zaleca się stosowanie pomiędzy Klientami pocztowymi nadawcy i adresata szyfrowania komunikacji w modelu end-to-end, ➤ w przypadku braku możliwości szyfrowania komunikacji w modelu end-to-end, zaleca się stosowanie szyfrowania przez nadawcę całej wiadomości e-mail (zapoznanie się adresata jest możliwe na serwerze dostawcy Klienta pocztowego nadawcy), ➤ w przypadku braku powyższej możliwości lub rezygnacji z takiej formy zabezpieczeń (np. z uwagi na ustalenia z adresatem), zaleca się szyfrowanie i hasłowanie załączników wiadomości e-mail (wraz z przekazaniem odrębnym kanałem komunikacyjnym hasel dostępu). <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ korzystanie z usług poczty elektronicznej w standardach innych niż biznesowe i bez zawarcia stosownej DPA, np. darmowych; ➤ w przypadku konieczności przesyłania informacji objętych Tajemnicą zawodową obrońcą nie zaleca się w tym celu korzystania ani z korespondencji e-mail ani komunikatorów ani usług internetowych przesyłania dużych paczek danych.
8.9 8.10 8.11	Korzystanie z Usług Online zapewniających możliwość kontroli logów	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ korzystanie z narzędzi umożliwiających monitoring/audyt logów (o ile jest to możliwe)

	<p>i dostępów.</p> <p>Korzystanie z Usług Online wyłącznie w standardzie biznesowym.</p> <p>Przechowywanie (retencja) danych na terytorium EOG.</p>	<p>z uwagi na możliwości funkcjonalne Usługi Online),</p> <ul style="list-style-type: none"> ➤ w przypadku przetwarzania przez Kancelarię danych w Usługach Online – wykorzystywanie w tym celu wyłącznie zaufanych Dostawców Usług Chmurowych, ➤ korzystanie z Usługi Online – wyłącznie w standardzie biznesowym, wraz z zawarciem stosownego DPA, uwzględniającego ewentualne przetwarzanie danych osobowych należących do szczególnych kategorii danych w rozumieniu RODO i Tajemnicy zawodowej, ➤ regularne wykonywanie dodatkowej lokalnej kopii zapasowej danych zgromadzonych w Usługach Online, ➤ stworzenie planu ciągłości działania Usługi Online i ewentualnego jej przywracania (wraz z odzyskiwaniem danych) na wypadek awarii, ➤ blokowanie udostępniania zasobów danych przetwarzanych w ramach Usługi Online bez dodatkowej autoryzacji. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ przetwarzanie w Usługach Online danych objętych Tajemnicą zawodową obrońcą bez dodatkowego szyfrowania danych w sposób uniemożliwiający zapoznanie się z tymi danymi Dostawcy Usługi Online, ➤ przetwarzanie danych poza terytorium EOG, <u>z zastrzeżeniem że, w przypadku konieczności wyboru miejsca przetwarzania danych poza terytorium EOG należy w pierwszej kolejności rozpatrzyć możliwość przetwarzania na terytorium EFTA lub terytorium UK (z wyłączeniem terytoriów zależnych).</u>
<p>9.3 9.4 9.5</p>	<p>Przekazywanie danych poza Kancelarię przy wykorzystaniu Usług Chmurowych w standardzie biznesowym.</p> <p>Przekazywanie danych</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ aby ewentualne przekazywanie przez Kancelarię danych objętych Tajemnicą zawodową poza Kancelarię (w tym klientom) nastąpiło wyłącznie przy zachowaniu właściwych standardów bezpieczeństwa

	<p>poza Kancelarię przy wykorzystaniu narzędzi lub usług darmowych, w tym niezapewniających standardów biznesowych i standardów ochrony danych osobowych.</p> <p>Przekazywanie danych poza Kancelarię na nośnikach danych bez hasła dostępu.</p>	<p>i z zapewnieniem ochrony Tajemnicy zawodowej,</p> <ul style="list-style-type: none"> ➤ udostępnienia danych przy wykorzystaniu Usługi Chmurowej, której subskrybentem jest Kancelaria lub na nośnikach danych zabezpieczonych silnym hasłem dostępu, ➤ szyfrowanie przekazywanych danych wraz z silnym hasłem dostępowym. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ udostępnianie danych poufnych przy wykorzystaniu darmowych narzędzi i usług, niespełniających standardów biznesowych i bez zawarcia stosownej DPA, ➤ udostępnienia danych na płytach CD/DVD-RW, na dyskach zewnętrznych lub pendrive'ach bez odpowiedniego szyfrowania. <p>W przypadku oczekiwania klienta Kancelarii do przekazania mu danych go dotyczących w sposób sprzeczny z zasadami bezpieczeństwa (w szczególności bez szyfrowania danych lub zabezpieczenia hasłem), zalecane jest uzyskanie przez Kancelarię potwierdzenia wydania takiej dyspozycji przez klienta, po uprzednim ogólnym poinformowaniu klienta o możliwych ryzykach z tym związanych.</p>
<p>10.4 10.5 10.6 10.7</p>	<p>Korzystanie z usług/najm u biur serwisowanych, jeśli nie zapewniają właściwych standardów bezpieczeństwa pozwalających na utrzymanie poufności danych znajdujących się w posiadaniu Kancelarii, w tym informacji objętych Tajemnicą zawodową.</p> <p>Korzystanie z ogólnodostępnego</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ aby dostęp do miejsca przechowywania dokumentów i sprzętów Kancelarii był nadzorowany i ograniczony do Personelu, z zastrzeżeniem, że klucze/karty wejściowe do pomieszczeń zajmowanych przez Kancelarię nie powinny być wykorzystane przez administratora biura lub wynajmującego bez uprzedniego poinformowania Kancelarii i wyłącznie w przypadkach zdarzeń dotyczących bezpieczeństwa biura i budynku; ➤ wprowadzenie polityki czystego biurka (po zakończonej pracy wszelkie dokumenty i sprzęt przenośny powinien być przechowywany

	<p>sprzętu komputerowego.</p> <p>Korzystanie z ogólnodostępnego serwera.</p> <p>Skanowanie lub drukowanie na sprzęcie ogólnodostępnym.</p>	<p>w zamkniętych bezpiecznych szafach), do których dostęp jest możliwy wyłącznie dla osób upoważnionych przez Kancelarię);</p> <ul style="list-style-type: none"> ➤ szyfrowanie komunikacji i danych przetwarzanych w sieci informatycznej biura serwisowanego (z zastrzeżeniem, że nie zaleca się korzystania z sieci wi-fi udostępnianego przez takie biuro); ➤ w przypadku drukowania dokumentów na drukarce udostępnionej przez biuro, stosowanie wyłącznie druku bezpiecznego (PIN/Follow-Me Printing) tj. systemu zabezpieczającego wydruki w ten sposób, że druk jest możliwy dopiero gdy użytkownik (osoba uprawniona) podejdzie do drukarki i dokona uwierzytelnienia np. poprzez wpisanie PINu, użycie karty zbliżeniowej, etc. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ korzystanie z usług/najmu biur serwisowanych, jeśli nie zapewniają właściwych dla danej kategorii przetwarzanych danych standardów bezpieczeństwa pozwalających na utrzymanie poufności danych znajdujących się w posiadaniu Kancelarii, w tym informacji objętych Tajemnicą zawodową (Kancelaria powinna dokonać w tym zakresie oceny i podjąć odpowiednie środki w celu zapewnienia tych standardów), ➤ korzystanie z ogólnodostępnej sieci wi-fi, komputera lub serwera zapewnianych przez administratora biura lub wynajmującego; ➤ skanowanie lub drukowanie dokumentów objętych Tajemnicą zawodową na ogólnodostępnym sprzęcie zapewnianym przez administratora biura lub wynajmującego, ➤ zlecanie czynności związanych z obiegiem dokumentów obsłudze biura serwisowanego (czynności te powinny być realizowane wyłącznie przez pracowników kancelarii).
1.7	Regularne szkolenia w zakresie wdrożonych	<u>Zalecane jest:</u>

	<p>polityk bezpieczeństwa i zasad korzystania ze sprzętu i usług.</p>	<ul style="list-style-type: none"> ➤ aby Adwokat posiadał podstawową wiedzę z zakresu korzystania z rozwiązań informatycznych wykorzystywanych przez Kancelarię, w tym w zakresie cyberzagrożeń, ➤ aby Adwokat odbywał regularne szkolenia z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa.
<p>12.1 12.2 12.3 12.4 12.5</p>	<p>Korzystanie z usług zewnętrznego wsparcia informatycznego wyłącznie przy zachowaniu zasad bezpieczeństwa, w tym poufności danych znajdujących się w posiadaniu Kancelarii.</p> <p>Powierzenie funkcji Administratora Systemów Informatycznych zewnętrznemu dostawcy usług.</p> <p>Zawarcie DPA.</p> <p>Wsparcie lokalne w biurze Kancelarii.</p> <p>Wsparcie z dostępem zdalnym bez stałej kontroli dostępu przez członka Personelu Kancelarii.</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ korzystanie z usług zewnętrznego wsparcia informatycznego wyłącznie przy zachowaniu zasad bezpieczeństwa, w tym poufności danych znajdujących się w posiadaniu Kancelarii, ➤ w przypadku korzystania z zewnętrznego wsparcia informatycznego w ramach, którego dostawca uzyskuje lub może uzyskać dostęp do danych osobowych – zawarcie stosownego DPA, ➤ aby wsparcie było świadczone w biurze Kancelarii i pod nadzorem, ➤ w przypadku korzystania ze wsparcia świadczonego w sposób zdalny nadzorowanie czynności członka personelu usługodawcy, ➤ przeprowadzanie dokładnej weryfikacji gdzie fizycznie znajdują się dane ze środowiska cyfrowego kancelarii w trakcie świadczenia usług wsparcia zewnętrznego. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ korzystanie ze wsparcia świadczonego w sposób zdalny bez stałej kontroli dostępu przez członka Personelu Kancelarii; ➤ korzystanie z dostawców wykorzystujących narzędzia do trenowania modeli AI w oparciu o treści dostarczane przez użytkownika.
<p>1.4</p>	<p>Zapewnienie fizycznych zabezpieczeń dostępu do miejsc przechowywania sprzętu i nośników danych.</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ aby dostęp do miejsca przechowywania dokumentów i sprzętów Kancelarii był nadzorowany i ograniczony do kręgu osób upoważnionych, z zastrzeżeniem, że

		<p>klucze/karty wejściowe do pomieszczeń zajmowanych przez Kancelarię nie powinny być wykorzystane przez administratora biura lub wynajmującego bez uprzedniego poinformowania Kancelarii i wyłącznie w przypadkach zdarzeń dotyczących bezpieczeństwa biura i budynku,</p> <p>➤ w trakcie transportu sprzęt i nośniki danych powinny zostać w sposób właściwy zabezpieczone przed dostępem osób nieuprawnionych.</p>
1.5	Korzystanie ze sprzętu należącego do osób trzecich, w szczególności przy dostępie do informacji objętych Tajemnicą zawodową.	<p><u>Zalecane jest:</u></p> <p>➤ korzystanie wyłącznie ze sprzętu służbowego Kancelarii w celach zawodowych celem zminimalizowania kręgu osób, które mogą mieć dostęp do Tajemnicy zawodowej.</p> <p><u>Niezalecane jest:</u></p> <p>➤ korzystanie ze sprzętu należącego do osób trzecich, skanowania lub drukowania na takim sprzęcie, a w szczególności przy dostępie do informacji objętych Tajemnicą zawodową,</p> <p>➤ skanowanie lub drukowanie poza biurem na sprzęcie należącym do osób trzecich (w tym w kafejkach internetowych i biurach serwisowanych).</p>
1.8	Wykupienie ubezpieczenia w zakresie odpowiedzialności dotyczącej cyberbezpieczeństwa i RODO.	<p><u>Zalecane opcjonalnie jest:</u></p> <p>➤ wykupienie przez Kancelarię stosownego ubezpieczenia w zakresie odpowiedzialności Kancelarii za szkody spowodowane przez Incydenty.</p>
14.2 14.3 14.4 14.5 14.6	Przygotowanie planu reagowania na Incydenty w formie checklisty. Monitorowanie oraz rejestrowanie nietypowych i podejrzanych zdarzeń.	<p><u>Zalecane jest:</u></p> <p>➤ monitorowanie i rejestrowanie zdarzeń, stanowiących odstępstwo od normalnego funkcjonowania systemów informatycznych, które mogą świadczyć o trwającym Incydencie,</p> <p>➤ sprawdzanie na publicznych portalach dostępnych w sieci, czy dane autoryzacyjne</p>

14.7	<p>Okresowe weryfikowanie możliwości wycieku używanych danych autoryzacyjnych przy pomocy publicznie dostępnych portali.</p> <p>Zgłoszenie wystąpienia Incydentu odpowiednim organom nadzorczym, klientom i innym zainteresowanym podmiotom w zakresie przewidzianym przepisami.</p> <p>Wykonanie analizy Incydentu po jego wystąpieniu, w celu wyciągnięcia wniosków, przeglądu zabezpieczeń i aktualizacji wdrożonych procedur bezpieczeństwa.</p> <p>Przywrócenie normalnego działania Kancelarii po wystąpieniu Incydentu bez przeglądu i aktualizacji zabezpieczeń i wdrożonych procedur.</p>	<p>używane w Kancelarii (m.in. loginy, hasła, e-maile) nie są częścią bazy danych objętych znanym wyciekiem,</p> <ul style="list-style-type: none"> ➤ aby w razie wystąpienia Incydentu zweryfikować obowiązek zakomunikowania tego zdarzenia podmiotom zainteresowanym, w szczególności Prezesowi Urzędu Ochrony Danych Osobowych, czy klientom, ➤ przeprowadzenie analizy Incydentu w celu ustalenia jego przyczyn oraz przebiegu, w celu wyciągnięcia wniosków na przyszłość. Wnioski te powinny stanowić podstawę do przeglądu istniejących zabezpieczeń i ewentualnej analizy wdrożonych procedur bezpieczeństwa. Jeżeli Personel nie posiada wiedzy lub narzędzi do przeprowadzenia takiej analizy zalecane jest skorzystanie z wsparcia zewnętrznych ekspertów. <p><u>Zalecane opcjonalnie jest:</u></p> <ul style="list-style-type: none"> ➤ opracowanie i wdrożenie planu reagowania na Incydeny, który będzie obejmował podstawowe kroki, które należy podjąć w razie stwierdzenia wystąpienia Incydentu. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ przywrócenie normalnego funkcjonowania Kancelarii po Incydencie, np. przez odtworzenie danych z kopii zapasowych, bez przeprowadzenia analizy Incydentu, co może prowadzić do ponownego wystąpienia Incydentu.
------	--	---

⁵ Ochrona punktów końcowych.

⁶ Wyskakujące okna na stronie internetowej nad, pod i przed treścią wyświetlaną na stronie internetowej. Z reguły wykorzystywane są w celach reklamowych lub informacyjnych.

ROZDZIAŁ II. ZALECENIA DODATKOWE

dedykowane dla Kancelarii małych, średnich i dużych

NUMER ZALECENIA	CZEGO DOTYCZY?	WYJAŚNIENIA
1.1	Korzystanie wyłącznie z licencjonowanego i aktualnego oprogramowania przeznaczonego do komercyjnego zastosowania.	<u>Zalecane jest:</u> <ul style="list-style-type: none">➤ w przypadku Kancelarii małych (posiadających wykwalifikowane stałe wsparcie informatyczne) oraz średnich i dużych – stosowanie zcentralizowanego aktualizowania oprogramowania lub aplikacji na urządzeniach mobilnych przy wykorzystaniu aplikacji do zarządzania urządzeniami (MDM).
1.3	Korzystanie z rozwiązań i usług informatycznych tylko od zaufanych dostawców, posiadających siedzibę na terytorium EOG, którzy umożliwiają (gdy dochodzi do powierzenia przetwarzania danych osobowych) zawarcie stosownej DPA, a także przetwarzających powierzone dane na terytorium EOG.	<u>Zalecane jest:</u> <ul style="list-style-type: none">➤ wdrożenie polityki wyboru rozwiązań, usług i dostawców wraz z określeniem minimalnych wymogów technicznych i prawnych uwzględnianych przy ich wyborze przez Kancelarię zgodnie z oceną ryzyka przetwarzania danych.
1.6	Okresowy przegląd cyberzagrożeń i dostosowanie stosownych środków technicznych i organizacyjnych przy uwzględnieniu istniejących i potencjalnych ryzyk.	<u>Zalecane jest:</u> <ul style="list-style-type: none">➤ przeprowadzanie okresowych przeglądów i audytów wewnętrznych wymagań dla wykorzystywanych rozwiązań i sprzętu, z uwagi na zmieniającą się technikę informatyczną;➤ przegląd ryzyk cyberbezpieczeństwa prowadzony regularnie, nie rzadziej niż raz w roku, oraz po każdym incydencie bezpieczeństwa. Wyniki analizy powinny być dokumentowane w rejestrze ryzyk, obejmującym identyfikację zagrożeń, ich ocenę oraz podjęte środki ograniczające;

		<ul style="list-style-type: none"> ➤ w przypadku kancelarii średnich i dużych wdrożenie uproszczonego planu reagowania na incydenty (Incident Response Plan), określającego procedury zgłaszania, eskalacji i komunikacji w razie naruszenia bezpieczeństwa, ➤ dostosowanie stosowanych środków technicznych i organizacyjnych przy uwzględnieniu istniejących i potencjalnych ryzyk dla bezpieczeństwa danych przetwarzanych przez Kancelarię, ➤ stosowanie modelu PDCA (Plan-Do-Check-Act), podejścia Privacy by Design i Security by Design.
2.3 3.3 4.3 6.3 7.3 8.3 11.3	Przeprowadzanie okresowej zmiany haseł.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ przeprowadzanie okresowej zmiany haseł, nie rzadziej niż co 1 miesiąc, przy czym decyzja w tym przedmiocie powinna uwzględniać przyjętą w Kancelarii klasyfikację przetwarzanych informacji oraz wdrożone procedury, ➤ aby decyzja o okresowej zmianie haseł lub jej częstotliwość uwzględniona była we wdrożonych procedurach bezpieczeństwa oraz systemie zarządzania bezpieczeństwem informacji.
15.1	Stosowanie polityki zarządzania konfiguracją, dostępem oraz monitorowaniem dostępu i sieci.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ w przypadku Kancelarii małych (posiadających wykwalifikowane stałe wsparcie informatyczne), średnich i dużych – wdrożenie polityki zarządzania dostęпами do systemów, aplikacji i sprzętu Kancelarii, wraz z narzędziami umożliwiającymi monitoring/audyt logów (o ile jest to możliwe z uwagi na możliwości funkcjonalne wykorzystywanych systemów, aplikacji i sprzętu), ➤ aby przydzielane użytkownikom loginy były zindywidualizowane, tj. przypisane tylko do jednego użytkownika i w sposób zapewniający jego identyfikację,

		<ul style="list-style-type: none"> ➤ aby użytkownik otrzymał określony dostęp do zasobów infrastruktury Kancelarii w minimalnym zakresie i tylko przez okres jaki jest zasadny z perspektywy podejmowanych czynności i realizacji procesów organizacyjnych Kancelarii, ➤ w przypadku Kancelarii małych, średnich i dużych – wprowadzenie klasyfikacji uprawnień i kategorii użytkowników, ➤ w przypadku Kancelarii małych (posiadających wykwalifikowane stałe wsparcie informatyczne), średnich i dużych – prowadzenie monitorowania sieci (w tym ruchu sieciowego i urządzeń sieciowych) wraz z automatycznym powiadomieniem o wykrytych zagrożeniach, ➤ w przypadku Kancelarii dużych – rozważenie korzystania z systemów detekcji anomalii IDPS (Intrusion Detection / Prevention System) oraz SIEM (Security Incident and Event Management), ➤ w przypadku Kancelarii średnich i dużych – rozważenie wprowadzenia segmentacji sieci wewnętrznej poprzez wydzielenie sieci VLAN (virtual local area network). <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ wykorzystywanie loginów, haseł lub służbowych adresów e-mail w innym celu niż związanym z świadczeniem usług i wykonywaniem zawodu, tj. nie zaleca się aby były one wykorzystywane w celach prywatnych (np. posłużenie się służbowym adresem e-mail do obsługi profilu prywatnego konta użytkownika na portalu Facebook). <p>W przypadku Kancelarii jednoosobowych stosowanie się do powyższych zaleceń może utrudnić funkcjonowanie Kancelarii bez istotnej poprawy poziomu bezpieczeństwa. Kancelarie tego typu powinny rozważyć (w przypadku posiadania niezbędnych kompetencji lub w przypadku planowanej zmiany ich statusu na Kancelarię małą) zasadność stosowania się do powyższych zaleceń.</p>
--	--	---

15.2	Wdrożenie w Kancelarii norm ISO z rodziny ISO/IEC 27000.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ wdrożenie w Kancelarii średniej i dużej norm ISO z rodziny ISO/IEC 27000 (wg wersji wybranej z przygotowanych przez Polski Komitet Normalizacyjny), a w szczególności: ISO/IEC 27000 (Technologia informacyjna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i słownictwo), ISO/IEC 27001 (Technologia informacyjna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania), ISO/IEC 27002 (Kontrola bezpieczeństwa informacji), ISO/IEC 27017 (Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczenia informacji na podstawie ISO/IEC 27002 dla usług w chmurze), ISO/IEC 27018 (Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady ochrony informacji o identyfikowalnych osobach (PII) w chmurach publicznych działających jako przetwarzający PII), ISO/IEC 27032 (Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dotyczące cyberbezpieczeństwa), ISO/IEC 27035 (Technika informatyczna – Zarządzanie incydentami w bezpieczeństwie informacji). <p>Uzyskanie certyfikatu zgodności z normami ISO nie jest konieczne. Wdrożenie ww. norm w Kancelarii małej jest zalecane opcjonalnie.</p>
15.3	Wdrożenie wewnętrznych polityk bezpieczeństwa w zakresie przetwarzania w Kancelarii informacji (w szczególności dotyczącej retencji danych), w tym danych objętych Tajemnicą zawodową.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ wdrożenie wewnętrznej polityki bezpieczeństwa przetwarzanych informacji, w szczególności zawierającej wytyczne dotyczące przetwarzania danych. W przypadku Kancelarii małych jest to zalecenie opcjonalne. <p>W przypadku wdrożenia polityki bezpieczeństwa przetwarzanych informacji Kancelaria powinna zidentyfikować kluczowe zasoby informacji, w szczególności informacje i dokumenty klientów,</p>

		<p>kluczowe usługi i rejestry/zbiory, które mają krytyczne znaczenie dla jego działalności. Ponadto, polityka powinna zawierać przy tym m.in.:</p> <ol style="list-style-type: none"> identyfikację potencjalnych zagrożeń i Incydentów (wraz z prawdopodobieństwem wystąpienia) oraz rozważeniem możliwych reakcji/środków, identyfikację procesów realizowanych w organizacji Kancelarii, politykę zarządzania siecią, sprzętem, usługami i uprawnieniami, stosowną dokumentację z zakresu ochrony danych osobowych (jeśli jest wymagana), klasyfikację i retencję informacji (z określeniem poziomów poufności), zasady pracy zdalnej i używania urządzeń mobilnych, korzystanie z usług i narzędzi sztucznej inteligencji (AI), w tym zakaz wprowadzania do nich informacji objętych tajemnicą zawodową, wymogi dotyczące autoryzacji dostępu i stosowania uwierzytelniania wieloskładnikowego (MFA).
15.4	Wdrożenie planu ciągłości działania istotnych elementów infrastruktury (usług) informatycznej Kancelarii i odzyskiwania danych (<i>data recovery</i>).	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ wdrożenie planu ciągłości działania istotnych elementów infrastruktury (usług) informatycznej Kancelarii i odzyskiwania danych (<i>data recovery</i>). W przypadku Kancelarii małych jest to zalecenie opcjonalne; ➤ plan ciągłości działania oraz odzyskiwania danych powinien być testowany co najmniej raz w roku lub po istotnej zmianie w infrastrukturze informatycznej. Zaleca się opracowanie prostego scenariusza reagowania na incydenty (np. cyberatak, awaria systemu, utrata nośnika), określającego osoby odpowiedzialne, procedurę komunikacji z klientami oraz sposób przywracania usług.
15.5	Regularne szkolenia Personelu w zakresie	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ prowadzenie szkoleń Personelu z zakresu

	wdrożonych polityk bezpieczeństwa i zasad korzystania ze sprzętu i usług.	<p>stosowanych w Kancelarii polityk i procedur, w szczególności dotyczących bezpieczeństwa informacji i cyberbezpieczeństwa,</p> <ul style="list-style-type: none"> ➤ szkolenia powinny być prowadzone przy rozpoczęciu współpracy oraz regularnie, nie rzadziej niż raz w roku. Rekomenduje się uzupełnienie szkoleń o moduły praktyczne, takie jak rozpoznawanie prób phishingu, bezpieczne korzystanie z chmury i AI, oraz postępowanie w razie incydentu bezpieczeństwa. Szkolenia powinny być dokumentowane i oceniane pod kątem skuteczności (np. krótkie testy wiedzy).
15.6	<p>Powierzenie administrowania i nadzoru nad infrastrukturą informatyczną Kancelarii osobie pełniącej funkcję Administratora</p> <p>Systemu Informatycznego (ASI).</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ powierzenie administrowania i nadzoru nad infrastrukturą informatyczną Kancelarii osobie pełniącej funkcję Administratora Systemu Informatycznego (ASI) na podstawie odpowiedniej umowy, ➤ w przypadku Kancelarii dużych – aby funkcję ASI pełnił wykwalifikowany członek Personelu. <p>W przypadku Kancelarii małych jest to zalecenie opcjonalne.</p>
15.7	<p>Posiadanie ubezpieczenia w zakresie odpowiedzialności</p> <p>dotyczącej cyberbezpieczeństwa i RODO.</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ wykupienie przez Kancelarię stosownego ubezpieczenia w zakresie odpowiedzialności Kancelarii za szkody spowodowane przez Incydenty.
15.8	<p>Aktualizacja oprogramowania przy wykorzystaniu środowiska testowego, w celu weryfikacji wpływu aktualizacji na działanie tych systemów i ewentualnego wykrycia podatności.</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ w przypadku Kancelarii dużych – przeprowadzanie aktualizacji oprogramowania istotnego z punktu widzenia podatności na Incydenty przy wykorzystaniu środowiska testowego, w celu weryfikacji wpływu aktualizacji na działanie tych systemów i ewentualnego wykrycia podatności, ➤ aktualizacje oprogramowania i systemów

		<p>powinny być wdrażane w sposób kontrolowany, zgodnie z procedurą zarządzania poprawkami (patch management), obejmującą m.in.:</p> <ul style="list-style-type: none"> a) ocenę wpływu aktualizacji na bezpieczeństwo i zgodność z politykami; b) testowanie w środowisku testowym; c) dokumentowanie wykonanych aktualizacji d) bieżące monitorowanie informacji o lukach bezpieczeństwa. <p>W przypadku Kancelarii małych i średnich jest to zalecenie opcjonalne.</p>
<p>16.1 16.2 16.3 16.4 17.1 17.2 17.3 18.1 18.2</p>	<p>Korzystanie przez Personel z prywatnego sprzętu w celach zawodowych.</p> <p>Korzystanie przez Personel w celach zawodowych wyłącznie ze sprzętu służbowego.</p> <p>Korzystanie z zewnętrznego serwisu IT w formie zdalnej bez bieżącego nadzoru członka Personelu.</p> <p>Stosowanie Hasła administratora.</p> <p>Prowadzenie ewidencji sprzętu powierzonego Personelowi.</p> <p>Wdrożenie polityki bezpieczeństwa.</p> <p>Monitoring i audyt śladowy.</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ stosowanie aplikacji do administracyjnego zarządzania urządzeniami (MDM), ➤ stosowanie Hasła administratora z pełnym dostępem do zasobów i ustawień systemu, deponowane w bezpiecznej kopercie w szafie pancernej. Pozwoli to zabezpieczyć dostęp do zasobów Kancelarii w przypadku zaistnienia Incydentu, ➤ w przypadku serwerów – stosowanie zasilania UPS, ➤ w przypadku serwerów kolokowanych u podmiotów trzecich zalecane jest stosowanie redundancji łączy i narzędzi sieciowych, ➤ korzystanie przez Personel w celach zawodowych wyłącznie ze sprzętu służbowego; ➤ wdrożenie polityki bezpieczeństwa (w szczególności w przypadku eksploatacji serwera lokalnego), ➤ w przypadku korzystania z własnych lub kolokowanych serwerów – zapewnienie redundancji łączy i narzędzi sieciowych, co wiąże się z zapewnieniem utrzymania ciągłości działania infrastruktury serwerowej Kancelarii, a więc i możliwości działalności bieżącej (w przypadku przechowywania danych objętych Tajemnicą zawodową),

		<ul style="list-style-type: none"> ➤ stosowanie narzędzi i rozwiązań służących do ochrony danych poufnych DLP (<i>Data Loss Prevention</i>), które pozwolą na ochronę wrażliwych informacji i automatyczne wykrywanie i blokowanie nieuprawnionego ujawnienia informacji, ➤ w celu przeciwdziałania nieuprawnionemu ujawnieniu informacji w obszarze DLP, należy określić wrażliwości danych i ich poziom zabezpieczenia, reguły dostępu do wrażliwych informacji i kontrolę tego, kto je ujawnia, ➤ należy szyfrować wrażliwe dane, aby uniemożliwić ich odczyt w przypadku wycieku. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ aby serwery własne, serwery kolokowane i hostowane, a także serwery wykorzystywane przez Dostawcę Usługi Chmurowej znajdowały się poza terytorium EOG (jeśli jednak dane będą przechowywane poza EOG, to niezbędne jest zawarcie stosownej DPA zgodnej z właściwymi aktami prawnymi, w tym Decyzją Wykonawczą Komisji (UE) 2021/914), ➤ stosowanie polityki korzystania przez Personel w celach zawodowych z prywatnego sprzętu (tzw. BYOD), ➤ korzystanie z zewnętrznego serwisu IT w formie zdalnej bez bieżącego nadzoru członka Personelu, ➤ w przypadku awarii sprzętu – przekazywanie sprzętu do serwisu (bez usunięcia danych) bez nadzoru członka Personelu.
19.1	Korzystanie z własnego serwera pocztowego.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ w przypadku Kancelarii dużych – korzystanie z własnego serwera pocztowego, co jednak wymaga posiadania odpowiednich zasobów i kompetencji; w przypadku Kancelarii średnich jest do zalecenie opcjonalne, ➤ blokowanie możliwości (bez autoryzacji) przesyłania przez członka Personelu za pośrednictwem korespondencji e-mail

		<p>większych paczek danych,</p> <ul style="list-style-type: none"> ➤ wprowadzenie możliwości dokonywania przez Personel zgłoszeń podejrzanych wiadomości e-mail obejmowanych automatycznie kwarantanną (przed ich analizą przez administratora).
20.1 21.1 22.1	Wdrożenie polityki wydawania danych uprawnionym organom w przypadkach określonych przepisami prawa.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ wdrożenie polityki dostępu i wydawania danych uprawnionym organom w przypadkach określonych przepisami praw; w szczególności zawierających procedurę zapewnienia zachowania Tajemnicy zawodowej.
23.1	Korzystanie z usług podmiotu posiadającego zweryfikowaną wiedzę z zakresu rozwiązań sieciowych i ISO z rodziny ISO/IEC 27000.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ w przypadku Kancelarii średnich i dużych – korzystanie z usług podmiotu posiadającego zweryfikowaną wiedzę z zakresu rozwiązań sieciowych i ISO z rodziny ISO/IEC 27000. <p>W przypadku Kancelarii małych jest to zalecenie opcjonalne.</p>
24.1 24.2 24.3 24.4 24.5 24.6 24.7	<p>Wdrożenie polityki zarządzania Incydentami.</p> <p>Prowadzenie rejestru Incydentów.</p> <p>Wyznaczenie zespołu reagowania na Incydenty, w tym zdefiniowanie ról i odpowiedzialności poszczególnych osób.</p> <p>Powierzenie zadań zespołu reagowania na Incydenty w całości zewnętrznemu dostawcy.</p> <p>Opracowanie planów komunikacji z klientami, mediami lub innymi podmiotami</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> ➤ ustanowienie w Kancelarii polityki zarządzania incydentami, strukturyzującej przyjęte w Kancelarii podejście do zapobiegania, identyfikowania, reagowania, klasyfikowania oraz analizowania Incydentów. Opracowane w Kancelarii wytyczne w zakresie klasyfikowania Incydentów powinno uwzględniać faktyczny lub potencjalny wpływ poszczególnych rodzajów Incydentów na poufność, autentyczność, integralność i dostępność danych przetwarzanych w systemach informatycznych, a także konieczność zgłoszenia wystąpienia Incydentu odpowiednim organom i zainteresowanym podmiotom, ➤ prowadzenie rejestru incydentów, który będzie obejmował datę wystąpienia Incydentu, dotknięte nim systemy, jego przebieg, przyczyny oraz wnioski z jego analizy,

	<p>zainteresowanymi na wypadek wystąpienia Incydentu.</p> <p>Okresowy przegląd darknetu pod kątem potencjalnych wycieków danych lub korzystanie z usług podmiotu świadczącego tego typu usługi.</p> <p>Okresowe przeprowadzanie szkoleń obejmujących ćwiczenia z wystąpienia Incydentu</p>	<ul style="list-style-type: none"> ➤ wyznaczenie zespołu reagowania na Incydynty (IRT), w tym zdefiniowanie ról i odpowiedzialności poszczególnych osób. Zaleca się, by członkami takiego zespołu byli co najmniej przedstawiciele najwyższego kierownictwa Kancelarii (np. Partnerzy Zarządzający), administrator systemów informatycznych oraz osoba odpowiedzialna za komunikację z podmiotami zewnętrznymi (w tym za przygotowanie ewentualnego zgłoszenia do PUODO). Zespół reagowania na Incydynty może być wspierany przez zewnętrznego usługodawcę. <p>W przypadku małych Kancelarii to zalecenie jest opcjonalne.</p> <ul style="list-style-type: none"> ➤ opracowanie planów komunikacji o wystąpieniu Incydentu z klientami, mediami lub innymi podmiotami zainteresowanymi. <p><u>Zalecane opcjonalnie jest:</u></p> <ul style="list-style-type: none"> ➤ okresowy przegląd znanych stron w darknetcie pod kątem potencjalnych wycieków mogących obejmować dane przetwarzane przez Kancelarię lub zlecenie wykonania tego typu usług zewnętrznemu dostawcy, ➤ uwzględnienie w planach szkoleń Personelu ćwiczeń symulujących wystąpienie Incydentu. <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> ➤ powierzenie utworzenia zespołu reagowania na Incydynty w całości zewnętrznemu podmiotowi, bez udziału Personelu.
--	--	--

Załącznik numer 2 do Dobrych Praktyk dotyczących cyberbezpieczeństwa w działalności kancelarii adwokackich i pracy Adwokata

ZALECENIA DODATKOWE KWARTALNY SELF-CHECK BEZPIECZEŃSTWA PRACY ZDALNEJ

Załącznik stanowi narzędzie pomocnicze służące do okresowej, samodzielnej oceny poziomu bezpieczeństwa środowiska pracy zdalnej. Zaleca się jego stosowanie nie rzadziej niż raz na kwartał, w celu weryfikacji zgodności z podstawowymi wymaganiami w zakresie cyberbezpieczeństwa oraz utrzymania właściwej higieny cyfrowej. Lista ma charakter orientacyjny i powinna być traktowana jako element wspierający rozwój kultury bezpieczeństwa, a nie formalny audyt.

Obszar	Pytanie kontrolne / wymóg	Tak <input type="checkbox"/>	Nie <input type="checkbox"/>	Uwagi
VPN	Czy profil VPN łączy się automatycznie i blokuje ruch poza tunelem (funkcja <i>kill-switch</i>)?			
Router domowy	WPA3 włączone; WPS wyłączony; brak zdalnego dostępu administracyjnego; silne i unikalne hasło administratora.			
Sieci	Czy urządzenia służbowe korzystają z osobnego SSID? Urządzenia IoT działają wyłącznie w sieci gościnniej?			
Systemy	Czy dysk jest zaszyfrowany, system i aplikacje aktualne, a oprogramowanie EDR/AV aktywne?			
Urządzenia mobilne (MDM/MAM)	Czy urządzenia mobilne spełniają politykę bezpieczeństwa (PIN/biometria, szyfrowanie, brak root/jailbreak)?			
Poczta i komunikatory	Czy używane są wyłącznie narzędzia z białej listy, z aktywnym E2EE i połączeniem VPN?			
Backup	Czy kopia zapasowa została wykonana i zaszyfrowana, a test przywracania zakończył się powodzeniem?			
Dostępy	Czy przeprowadzono przegląd uprawnień i usunięto konta nieużywane (zasada najmniejszych uprawnień)?			
Bezpieczeństwo fizyczne	Czy ekran nie jest widoczny z zewnątrz, użyto filtra prywatyzującego, a blokada ekranu aktywuje się po bezczynności?			
Reakcja na incydenty	Czy plan reagowania jest aktualny, a dane kontaktowe wsparcia są pod ręką?			

LISTA KONTROLNA WIDEO-ROZPRAW/SPOTKAŃ ONLINE

Załącznik ma na celu wsparcie adwokatów w zapewnieniu odpowiedniego poziomu bezpieczeństwa i poufności podczas uczestnictwa w wideorozprawach oraz spotkaniach online. Lista kontrolna pozwala na weryfikację kluczowych elementów technicznych i organizacyjnych, które minimalizują ryzyko nieuprawnionego dostępu do informacji objętych tajemnicą zawodową. Zaleca się jej stosowanie każdorazowo przed rozpoczęciem wideospotkania o charakterze zawodowym.

Obszar	Pytanie kontrolne / wymóg	Tak <input type="checkbox"/>	Nie <input type="checkbox"/>	Uwagi
Środowisko	Czy tło jest neutralne, bez widocznych dokumentów lub danych? Czy w pomieszczeniu przebywają wyłącznie osoby uprawnione? Czy urządzenia potencjalnie podsłuchujące (np. asystenci głosowi, urządzenia IoT) są wyłączone lub odłączone od sieci pracy?			
Łącze	Czy połączenie VPN jest aktywne? Czy wykonano test prędkości i opóźnień? Czy korzystasz z przewodowego połączenia internetowego lub prywatnego hotspotu LTE/5G zamiast publicznej sieci Wi-Fi?			
Aplikacja	Czy wykorzystywane narzędzie pochodzi z białej listy i zapewnia szyfrowanie (E2EE lub co najmniej <i>in transit</i>)? Czy spotkanie zabezpieczono hasłem lub <i>waiting room</i> ? Czy funkcja automatycznego nagrywania jest wyłączona (chyba że nagrywanie zostało uzasadnione i uzgodnione)?			
Urządzenia	Czy kamera i mikrofon działają poprawnie, a oprogramowanie urządzenia jest aktualne? Czy zamknięto wszystkie zbędne aplikacje działające w tle?			
Higiena informacji	Czy podczas udostępniania ekranu ograniczono widok wyłącznie do niezbędnego okna? Czy powiadomienia systemowe i komunikatorów są wyłączone?			
Po spotkaniu	Czy usunięto pliki tymczasowe i materiały z wideokonferencji? Czy połączenie VPN zostało zamknięte dopiero po zakończeniu pracy?			

Załącznik numer 3 do Dobrych Praktyk dotyczących cyberbezpieczeństwa w działalności kancelarii adwokackich i pracy Adwokata

LISTA KONTROLNA BEZPIECZEŃSTWA DOSTAWCY IT

Lista kontrolna bezpieczeństwa dostawcy IT stanowi narzędzie pomocnicze służące ocenie ryzyka przy wyborze, zmianie lub okresowym przeglądzie dostawcy usług informatycznych, w szczególności usług chmurowych, hostingu, poczty elektronicznej, systemów do zarządzania dokumentami, komunikatorów oraz usług serwisowych. Jej celem jest ułatwienie kancelariom adwokackim przeprowadzania wstępnego audytu bezpieczeństwa, a także udokumentowania należytej staranności w procesie zawierania umów z dostawcami technologii, zgodnie z zasadą *Security & Privacy by Design*.

Przed podpisaniem umowy lub odnowieniem współpracy zaleca się przejście przez listę pytań kontrolnych oraz udokumentowanie odpowiedzi dostawcy. Odpowiedzi te powinny umożliwiać identyfikację potencjalnych ryzyk oraz stanowić podstawę decyzji o akceptacji, warunkowej akceptacji bądź odrzuceniu dostawcy. Dokumentacja wypełnionej listy powinna być przechowywana w kancelarii jako element wewnętrznej dokumentacji bezpieczeństwa i może służyć jako dowód zachowania należytej staranności w przypadku incydentów lub audytów.

Ocena końcowa powinna polegać na przypisaniu każdemu z analizowanych obszarów (np. lokalizacja danych, szyfrowanie, reakcja na incydenty, zarządzanie dostępem) poziomu ryzyka: niskiego, średniego lub wysokiego. W przypadku wystąpienia ryzyka średniego lub wysokiego kancelaria powinna rozważyć jego ograniczenie przez wprowadzenie dodatkowych środków bezpieczeństwa albo zastrzeżeń umownych.

Zakres stosowania listy różni się w zależności od wielkości kancelarii:

- Kancelarie jednoosobowe i małe mogą korzystać z uproszczonej wersji listy (obejmującej najważniejsze pytania), prowadzonej w formie prostego arkusza lub pliku tekstowego.
- Kancelarie średnie i duże powinny traktować listę jako element formalnej procedury *Vendor Security Assessment* (oceny bezpieczeństwa dostawców), powiązanej z polityką zakupową, rejestracją dostawców i audytem IT.

W każdym przypadku rekomenduje się okresowy przegląd i aktualizację listy (co najmniej raz w roku lub po każdej istotnej zmianie w usługach dostawcy).

Lista kontrolna:

1. Podstawowe informacje o dostawcy

- Czy dostawca posiada siedzibę i centrum danych na terenie EOG (lub zapewnia równoważne gwarancje prawne)?
- Czy dostawca udostępnia dane identyfikujące podwykonawców (subprocesorów)?
- Czy w umowie znajdują się zapisy o poufności, ochronie danych i obowiązku zgłaszania incydentów bezpieczeństwa?

2. Certyfikaty i zgodność z normami

- Czy dostawca posiada aktualny certyfikat ISO/IEC 27001 lub równoważny?
- Czy stosuje normy lub praktyki branżowe (np. ENISA, NIST, CIS Controls)?
- Czy certyfikat obejmuje zakres usług, z których korzysta kancelaria?

3. Przetwarzanie i przechowywanie danych

- Gdzie fizycznie przetwarzane i przechowywane są dane?
- Czy dane są szyfrowane w spoczynku i podczas transmisji?
- Czy istnieje możliwość żądania usunięcia danych i ich kopii po zakończeniu współpracy?

4. Zarządzanie dostępem i kontami użytkowników

- Czy system dostawcy wspiera uwierzytelnianie wieloskładnikowe (MFA)?
- Czy kancelaria może samodzielnie zarządzać kontami użytkowników i poziomami dostępu?
- Czy logi dostępu są dostępne dla klienta (kancelarii)?

5. Reagowanie na incydenty

- Czy dostawca posiada plan reagowania na incydenty bezpieczeństwa (*Incident Response Plan*)?
- W jakim terminie zobowiązuje się do powiadomienia o incydencie?
- Czy kancelaria ma wskazaną osobę kontaktową ds. bezpieczeństwa?

6. Kopie zapasowe i ciągłość działania

- Czy dane są objęte automatycznym backupem?
- Jak długo przechowywane są kopie zapasowe i gdzie się znajdują?
- Czy dostawca deklaruje testowanie przywracania danych?

7. Sztuczna inteligencja i modele językowe (AI)

- Czy dostawca korzysta z narzędzi AI do przetwarzania danych klientów (np. analizy treści, uczenia modeli)?
- Czy dane kancelarii mogą być wykorzystywane do trenowania modeli?
- Czy istnieje klauzula *no-train* gwarantująca, że dane kancelarii nie są używane do uczenia algorytmów?

8. Monitoring i raportowanie

- Czy dostawca udostępnia raporty z audytów bezpieczeństwa lub testów penetracyjnych?
- Czy zapewnia dostęp do dzienników zdarzeń (logów) dla klienta?
- Czy kancelaria otrzymuje okresowe raporty o zmianach subprocesorów lub aktualizacjach zabezpieczeń?

Załącznik numer 4 do Dobrych Praktyk dotyczących cyberbezpieczeństwa w działalności kancelarii adwokackich i pracy Adwokata

NARZĘDZIE WSPIERAJĄCE ZASADĘ NALEŻYTEJ STARANNOŚCI I PODEJŚCIE OPARTE NA RYZYKU

1. Cel i zakres stosowania

Celem niniejszego załącznika jest przedstawienie prostego, praktycznego sposobu przeprowadzenia analizy ryzyka w kancelarii adwokackiej niezależnie od jej wielkości czy poziomu wiedzy technicznej. Analiza ryzyka pozwala na racjonalny dobór środków bezpieczeństwa, adekwatnych do charakteru przetwarzanych informacji, potencjalnych zagrożeń oraz skali działalności kancelarii.

Zgodnie z zasadą *Security & Privacy by Design*, identyfikacja ryzyk powinna następować zanim wdrożony zostanie nowy system, usługa lub proces (np. praca zdalna, komunikator, platforma do wideokonferencji). Dokumentacja przeprowadzonej analizy stanowi element potwierdzający należyte wykonywanie obowiązków zawodowych oraz zgodność z przepisami o ochronie danych osobowych. Analiza ryzyka nie jest procesem technicznym, lecz sposobem myślenia o bezpieczeństwie. Jej celem nie jest wyeliminowanie wszystkich zagrożeń, ale zrozumienie, które są najbardziej prawdopodobne i mają największe skutki, oraz wdrożenie środków, które realnie ograniczają te ryzyka.

2. Zasady ogólne – analiza ryzyka krok po kroku

Krok 1 – Określ, co chronisz (aktywa informacyjne)

Wypisz wszystkie kluczowe zasoby kancelarii, w tym dane, systemy i urządzenia, bez których nie można wykonywać pracy.

Przykłady: dokumentacja klientów, skrzynka e-mail, system do obsługi spraw, komputer przenośny, chmura, konto portalu informacyjnym sądów powszechnych, czy w e-KRS.

Krok 2 – Zidentyfikuj zagrożenia i podatności

Dla każdego zasobu pomyśl, co może pójść nie tak i dlaczego.

Przykłady: utrata laptopa w podróży, atak phishingowy i wyłudzenie hasła, błąd pracownika przy wysyłce dokumentu, awaria dysku lub utrata kopii zapasowej.

Krok 3 – Oceń ryzyko (prawdopodobieństwo i skutki)

Dla każdego zagrożenia określ prawdopodobieństwo jego wystąpienia (niskie, średnie, wysokie) oraz skutek w razie wystąpienia (mały, średni, poważny). Połącz te wartości, tworząc prostą macierz ryzyka i oznaczając, które obszary wymagają działań natychmiastowych.

Krok 4 – Określ działania ograniczające ryzyko

Dla każdego ryzyka wskaż działania ograniczające jego skutki.

Przykłady: szyfrowanie urzędzeń, kopie zapasowe, weryfikacja dostawcy IT, polityka haseł lub szkolenia pracowników.

Krok 5 – Dokumentuj i aktualizuj analizę

Analizę ryzyka należy aktualizować przynajmniej raz w roku lub po każdej istotnej zmianie w systemach, procesach lub personelu.

3. Prosty szablon analizy ryzyka

Nr	Aktywo / proces	Zagrożenie	Prawdopodobieństwo	Skutek	Ocena ryzyka	Środek ograniczający	Odpowiedzialny	Termin / status
1	Laptop adwokata	Kradzież lub utrata	Średnie	Poważny	Wysokie	Szyfrowanie dysku, hasło BIOS, 2FA do poczty	Adwokat	wdrożone
2	System DMS (chmura)	Błąd dostawcy / awaria	Niskie	Poważny	Średnie	Backup lokalny + klauzula SLA	Administrator IT	do wdrożenia
3	Poczta e-mail	Phishing	Wysokie	Średni	Wysokie	Filtry antyspam + szkolenie personelu	Wspólnik X	wdrożone

4. Interpretacja wyników

Po wypełnieniu tabeli kancelaria powinna zaakceptować ryzyka niskie, zaplanować działania dla ryzyk średnich, a dla ryzyk wysokich wdrożyć środki ograniczające lub zmienić procesy. Wskazane jest stosowanie prostej klasyfikacji kolorystycznej: niskie – zielone, średnie – żółte, wysokie – czerwone.

5. Rekomendacje wdrożeniowe wg skali kancelarii

- Kancelarie jednoosobowe lub małe mogą ograniczyć analizę do kluczowych ryzyk, aktualizowaną raz w roku.
- Kancelarie średnie powinny prowadzić pełną tabelę ryzyka z przypisaniem odpowiedzialnych osób. Kancelarie duże rekomenduje się, by wdrożyły prosty rejestr ryzyk powiązany z planem szkoleń, audytów i kopii zapasowych.