

DOBRE PRAKTYKI DOTYCZĄCE CYBERBEZPIECZEŃSTWA  
W DZIAŁALNOŚCI KANCELARII ADWOKACKICH  
I PRACY ADWOKATA

## WPROWADZENIE

Niniejszy dokument stanowi zbiór dobrych praktyk dotyczących cyberbezpieczeństwa w działalności kancelarii adwokackiej i pracy Adwokata. Dobre Praktyki mają charakter zaleceń, których stosowanie nie jest obligatoryjne a brak ich stosowania nie rodzi bezpośrednich negatywnych skutków w odpowiedzialności zawodowej czy dyscyplinarnej. Nie wyłącza to jednak 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.

Dobre Praktyki przedstawione w niniejszym dokumencie nie stanowią wyczerpującej listy zaleceń z zakresu 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.

Dobre Praktyki nie zawierają rekomendacji 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.

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).

Ze względu na różnice w skali występującego ryzyka oraz możliwości techniczne, organizacyjne i procesowe poszczególnych grup adresatów, przyjęto podział na następujące grupy kancelarii:

GRUPA	OPIS
<p><b>jednoosobowe (1-os.)</b></p>	<p>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. of Counsel) powinny być traktowane jako osoba trzecia, z którą należy zawrzeć odpowiednie umowy lub udzielić stosownych upoważnień.</p>
<p><b>Małe (2 – 10 os.)</b></p>	<p>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. of Counsel) powinny być traktowane jako osoba trzecia, z którą należy zawrzeć odpowiednie umowy lub udzielić stosownych upoważnień.</p>
<p><b>Średnie (11 – 20 os.)</b></p>	<p>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. of Counsel) 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.</p>
<p><b>Duże (powyżej 20 os.)</b></p>	<p>Kancelarie adwokackie prowadzone w dowolnej formie prawnej (jednoosobowe działalności gospodarcze, zespoły adwokackie, spółki</p>

	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. of Counsel) 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 wspólnikami 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. ENISA<sup>1</sup>).

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.

---

<sup>1</sup> European Union Agency for Cybersecurity.

## 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):

<b>Chmura Obliczeniowa</b>	pula współdzielonych, dostępnych na żądanie przez sieci teleinformatycznych, 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). <sup>2</sup>
<b>Dobre Praktyki</b>	niniejsze Dobre Praktyki dotyczące cyberbezpieczeństwa w działalności Kancelarii i pracy Adwokata.
<b>Dostawca Usług Chmurowych</b>	podmiot, który dysponuje infrastrukturą i oprogramowaniem służącym do świadczenia Usług Chmurowych oraz świadczy te usługi.
<b>Dostawca Usług Online</b>	podmiot, który prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową świadczy Usługi Online. Dostawcą Usług Online jest w szczególności Dostawca Usług Chmurowych.
<b>DPA</b>	umowa powierzenia przetwarzania danych osobowych, w tym zawierana poprzez akceptację regulaminu lub polityki przetwarzania danych osobowych dostawcy.
<b>EFTA</b>	Europejskie Stowarzyszenie Wolnego Handlu.
<b>EOG</b>	Europejski Obszar Gospodarczy.
<b>Hasło administratora</b>	hasło umożliwiające pełne zarządzanie systemem informatycznym, w tym nadawanie i odbieranie uprawnień poszczególnym użytkownikom.
<b>Kancelaria</b>	organizacja służąca wykonywaniu zawodu przez Adwokata, prowadzona w formie przewidzianej przepisami prawa (jednoosobowa działalność gospodarcza, zespół adwokacki,

<sup>2</sup> Za National Institute of Standards and Technology, Definition of cloud computing, Special Publication 800-145.

	spółka osobowa).
<b>Klient poczty</b>	aplikacja na urządzenie mobilne lub komputer stacjonarny służąca do obsługi korespondencji e-mail.
<b>Incydent</b>	zdarzenie, które stanowi naruszenie lub zagrożenie naruszenia poufności, integralności lub dostępności systemu informatycznego lub informacji, którą system przetwarza, w tym przechowuje lub przesyła lub które stanowi naruszenie lub zagrożenie naruszenia zasad bezpieczeństwa, procedur bezpieczeństwa, lub zasad dopuszczalnego korzystania. <sup>3</sup> Incydem jest w szczególności nieautoryzowane ujawnienie informacji, w tym informacji objętych Tajemnicą zawodową lub danych osobowych w rozumieniu RODO.
<b>Personel</b>	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).
<b>RODO</b>	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
<b>SaaS</b>	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. <sup>4</sup>
<b>Szyfrowanie „at rest”</b>	szyfrowanie danych „w spoczynku” (np. szyfrowanie przechowywanych plików, kopii zapasowych, informacji

<sup>3</sup> Za National Institute of Standards and Technology, Definition of security incident, Special Publication 800-128.

<sup>4</sup> Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy "Wspólna Infrastruktura Informatyczna Państwa".

	zgrupowanych w bazie danych).
<b>Szyfrowanie „in transit”</b>	szyfrowanie danych w trakcie transmisji (przesyłania) danych (np. podczas przesyłania danych w sieci teleinformatycznej, w tym z/do Chmury Obliczeniowej).
<b>Tajemnica zawodowa</b>	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.
<b>UK</b>	Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej, z wyłączeniem terytoriów zależnych.
<b>Usługi Chmurowe</b>	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.
<b>Usługi Online</b>	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.

## Dobre praktyki dotyczące cyberbezpieczeństwa w działalności kancelarii adwokackich i pracy Adwokata

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.

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 (dobrą praktyką jest stosowanie danego zalecenia),
- 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).

zalecane  
opcjonalne

ZO

zalecane

Z

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.



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 i aktualnego oprogramowania przeznaczonego do komercyjnego zastosowania.	Z
1.2	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
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.	Z
1.4	Zapewnienie fizycznych zabezpieczeń dostępu do miejsc przechowywania sprzętu i nośników danych.	Z
1.5	Korzystanie ze sprzętu należącego do osób trzecich, w szczególności przy dostępie do informacji objętych Tajemnicą zawodową.	N
1.6	Okresowy przegląd cyberzagrożeń i dostosowanie stosownych środków technicznych i organizacyjnych przy uwzględnieniu istniejących i potencjalnych ryzyk.	Z
1.7	Regularne szkolenia w zakresie wdrożonych polityk bezpieczeństwa i zasad korzystania ze sprzętu i usług.	Z
1.8	Posiadanie ubezpieczenia w zakresie odpowiedzialności dotyczącej cyberbezpieczeństwa i RODO.	ZO

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.	N
2.16	Przekazywanie sprzętu do naprawy (z danymi) bez nadzoru.	N
2.17	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

### 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), które nie są wykorzystywane w sposób stały i konieczny.	Z

3.16	Korzystanie z usług telekomunikacyjnych, których abonentem nie jest Kancelaria.	N
------	---	---

#### 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 dostępowych.	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 co najmniej WPA-2.	Z
5.6	Korzystanie wyłącznie z odpowiednio zabezpieczonych przeglądarek internetowych.	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 zaufanych dostawców, posiadających siedzibę na terytorium EOG, którzy umożliwiają (gdy dochodzi do powierzenia przetwarzania danych osobowych) zawarcie	Z

	stosownej DPA, a także przetwarzających powierzone dane na terytorium EOG.	
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

## 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).	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	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
8.8	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
8.9	Korzystanie z Usług Online zapewniających możliwość kontroli logów i dostępu.	Z
8.10	Korzystanie z Usług Online wyłącznie w standardzie biznesowym.	Z
8.11	Przechowywanie (retencja) danych na terytorium EOG.	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

#### 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

## ROZDZIAŁ II ZALECENIA DODATKOWE – KANCELARIE MAŁE, ŚREDNIE I DUŻE

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.

### 13. Zalecenia ogólne

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
13.1	Stosowanie polityki zarządzania konfiguracją, dostępem oraz monitorowaniem dostępu i sieci.	Z	Z	Z
13.2	Wdrożenie w Kancelarii norm ISO z rodziny ISO/IEC 27000.	ZO	Z	Z
13.3	Wdrożenie wewnętrznych polityk bezpieczeństwa w zakresie przetwarzania w Kancelarii informacji (w szczególności dotyczącej przechowywania danych), w tym danych objętych Tajemnicą zawodową.	ZO	Z	Z
13.4	Wdrożenie planu ciągłości działania istotnych elementów infrastruktury (usług) informatycznej Kancelarii i odzyskiwania danych (data recovery).	ZO	Z	Z
13.5	Regularne szkolenia Personelu w zakresie wdrożonych polityk bezpieczeństwa i zasad korzystania ze sprzętu i usług.	Z	Z	Z

13.6	Powierzenie administrowania i nadzoru nad infrastrukturą informatyczną Kancelarii osobie pełniącej funkcję Administratora Systemu Informatycznego (ASI).	ZO	Z	Z
13.7	Posiadanie ubezpieczenia w zakresie odpowiedzialności dotyczącej cyberbezpieczeństwa i RODO.	Z	Z	Z
13.8	Aktualizacja oprogramowania przy wykorzystaniu środowiska testowego, w celu weryfikacji wpływu aktualizacji na działanie tych systemów i ewentualnego wykrycia podatności.	ZO	ZO	Z

#### 14. Komputery PC i przenośne

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
14.1	Korzystanie przez Personel z prywatnego sprzętu w celach zawodowych.	N	N	N
14.2	Korzystanie przez Personel w celach zawodowych wyłącznie ze sprzętu służbowego.	Z	Z	Z
14.3	Korzystanie z zewnętrznego serwisu IT w formie zdalnej bez bieżącego nadzoru członka Personelu.	N	N	N
14.5	Wdrożenie stosowania Haseł administratora.	Z	Z	Z

#### 15. Smartfon

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
15.1	Korzystanie przez Personel z prywatnego sprzętu w celach zawodowych.	N	N	N
15.2	Korzystanie przez Personel w celach zawodowych wyłącznie ze sprzętu służbowego.	Z	Z	Z
15.3	Prowadzenie ewidencji sprzętu powierzonego Personelowi.	Z	Z	Z

#### 16. Serwery i urządzenia NAS

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
16.1	Opracowanie i wdrożenie formalnej polityki bezpieczeństwa informacji.	Z	Z	Z

#### 17. Poczta elektroniczna

Numer Zalecenia	Czynnik \ Adresat	małe	średnie	duże
17.1	Korzystanie z własnego serwera pocztowego.	N	ZO	Z

#### 18. Back-up

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

#### 19. Przetwarzanie danych w Usługach Online

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

#### 20. Przekazywanie danych poza Kancelarię, w tym do klienta

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

20.1	Wdrożenie polityki przekazywania danych w przypadkach określonych przepisami prawa.	Z	Z	Z
------	---	---	---	---

## 21. Obsługa zewnętrzna IT

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

## Załącznik nr 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 Dobrych Praktyk:

### ROZDZIAŁ I ZALECENIA PODSTAWOWE (dedykowane dla Kancelarii jednoosobowych, bazowe dla pozostałych grup Kancelarii)

NUMER ZALECENIA	CZEGO DOTYCZY?	WYJAŚNIENIA
1.1	Korzystanie wyłącznie z licencjonowanego i aktualnego oprogramowania przeznaczonego do komercyjnego zastosowania.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"><li>➤ korzystanie z oprogramowania na podstawie licencji do użytku komercyjnego uzyskanej od podmiotu uprawnionego i zgodnie z jej warunkami,</li><li>➤ 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),</li><li>➤ instalowanie aktualizacji oprogramowania bez zbędnej zwłoki, w szczególności w przypadku łat bezpieczeństwa udostępnionych w związku z wykryciem luk,</li><li>➤ stosowanie aktualizacji automatycznych lub wykorzystujących aktualizacje wymagające ustalenia z użytkownikiem czasu przeprowadzenia aktualizacji.</li></ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"><li>➤ korzystanie w celach zawodowych z oprogramowania przeznaczonego wyłącznie</li></ul>

		<p>do użytku osobistego lub edukacyjnego (np. freeware, shareware),</p> <ul style="list-style-type: none"> <li>➤ korzystanie w celach zawodowych ze sprzętu komputerowego wyposażonego w system operacyjny Windows w wersji innej niż PRO lub Enterprise,</li> <li>➤ korzystanie z nieautoryzowanych przez producenta oprogramowania modyfikacji oprogramowania (w szczególności w przypadku systemu operacyjnego przeznaczonego dla telefonów komórkowych typu smartphone),</li> <li>➤ instalowanie aplikacji mobilnych pobranych spoza autoryzowanych sklepów aplikacji (m.in. Google Store, Apple Store) lub ze źródeł nie pochodzących od producenta,</li> <li>➤ korzystanie z oprogramowania względem którego producent nie zapewnia wsparcia i aktualizacji.</li> </ul>
<p>2.1 3.1 4.1 6.1 7.1 8.1 9.1 11.1</p>	<p><b>Stosowanie silnych haseł dostępowych.</b></p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ 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.),</li> <li>➤ 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),</li> <li>➤ w przypadku dostępów w rzadko wykorzystywanych aplikacjach lub portalach – stosowanie jednorazowego losowo wybranego hasła (kolejne logowanie może nastąpić przy wykorzystaniu funkcji przypomnienia hasła),</li> <li>➤ stosowanie hasła dostępowego na komputerach na poziomie BIOS,</li> <li>➤ korzystanie (o ile jest to możliwe) z automatycznego blokowania dostępu w</li> </ul>

		<p>przypadku niepoprawnego podania hasła (np. po 3 nieudanej próbie logowania),</p> <ul style="list-style-type: none"> <li>➤ w przypadku bezczynności użytkownika (o ile jest to możliwe) – stosowanie automatycznego wylogowania z konta/usługi.</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ aby hasło bazowało na łatwo identyfikowalnych powiązaniach z osobą użytkownika, organizacją lub usługą, do której jest to dostęp,</li> <li>➤ udostępnianie innym osobom (w tym współpracownikom lub rodzinie) hasła do konta przypisanego do określonego użytkownika.</li> </ul>
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"> <li>➤ w przypadku korzystania z większej ilości haseł – korzystanie z menadżera haseł lub sprzętowych tokenów U2F.</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ stosowanie jednego hasła do kilku kont dostępowych; zwiększa to ryzyko kompromitacji hasła i w konsekwencji wycieku danych poufnych, w tym objętych Tajemnicą zawodową.</li> </ul>
2.3 3.3 4.3 6.3 7.3	Przeprowadzanie okresowej zmiany haseł lub stosowanie menadżera haseł.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ 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,</li> </ul>

<p>8.3 11.3</p>		<p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ przeprowadzanie zbyt częstej zmiany haseł (np. co kilka dni); skutkować to może utratą dostępu lub kompromitacją stosowanych haseł.</li> </ul>
<p>2.4 3.4 4.4 6.4 7.4 8.4 11.4</p>	<p>Stosowanie uwierzytelniania wieloskładnikowego (MFA).</p>	<p>Uwierzytelnianie wieloskładnikowe (MFA) zwiększa 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"> <li>➤ w przypadku, gdy jest to technicznie możliwe i dostępne – stosowanie uwierzytelniania wieloskładnikowego (MFA),</li> <li>➤ korzystanie z dostępnych aplikacji MFA.</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ wykorzystywanie w procesie wieloskładnikowego uwierzytelniania (poza hasłem) jedynie haseł/kodów dostępu przesyłanych w treści wiadomości tekstowych na numery telefonu komórkowego.</li> </ul>
<p>2.5 3.5 4.5 5.1 5.5</p>	<p>Stosowanie szyfrowania danych i komunikacji. Stosowanie szyfrowania wiadomości e-mail w przypadku braku szyfrowania komunikacji pomiędzy Klientami pocztowymi (programami pocztowymi).</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ korzystanie z komputerów wykorzystujących procesory wyposażone w moduł TPM lub spełniające podobne funkcje,</li> <li>➤ 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</li> </ul>



<p>6.5 6.6 7.5 8.5 8.6 9.2 10.1 11.5</p>	<p>Stosowanie szyfrowania lub hasłowania załączników wiadomości e-mail. Szyfrowanie kopii zapasowej danych. W przypadku korzystania z Usług Online wybór tych Usług Online, których dostawca zapewnia szyfrowanie komunikacji i danych. Stosowanie dodatkowego (własnego) szyfrowania danych przetwarzanych w ramach Usługi Chmurowej. Stosowanie szyfrowania danych i komunikacji w przypadku wykorzystywania sieci dostarczanej w ramach usługi biura serwisowanego. Korzystanie z komunikatorów niezapewniających szyfrowania danych i komunikacji typu end-to-end.</p>	<p>operacyjnym macOS zalecane jest aktywowanie funkcjonalności FileVault),</p> <ul style="list-style-type: none"> <li>➤ szyfrowanie danych znajdujących się w posiadaniu Kancelarii (w szczególności objętych Tajemnicą zawodową obrońcą),</li> <li>➤ szyfrowanie z poziomu ustawień BIOS wraz z hasłem dostępowym na poziomie BIOS,</li> <li>➤ szyfrowanie danych objętych Tajemnicą zawodową przy wykorzystaniu co najmniej algorytmu AES 128 bit z kluczem 256 bitowym,</li> <li>➤ stosowanie (o ile jest to możliwe) szyfrowania komunikacji end-to-end, a w przypadku braku możliwości stosowania tej metody, zaleca się stosowanie Szyfrowania „in transit” (wraz z Szyfrowaniem „at rest” przechowywanych danych),</li> <li>➤ szyfrowanie kopii zapasowych (back-up) danych,</li> <li>➤ szyfrowanie całej wiadomości e-mail w przypadku braku szyfrowania komunikacji pomiędzy Klientami pocztowymi,</li> <li>➤ szyfrowanie lub hasłowanie załączników do wiadomości e-mail,</li> <li>➤ 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),</li> <li>➤ 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, przy czym nie gorsze niż w standardzie WPA-2),</li> </ul>
--	--	--

		<ul style="list-style-type: none"> <li>➤ w przypadku korzystania z narzędzi służących do wideokonferencji zaleca się stosowanie tych zapewniających szyfrowanie komunikacji end-to-end lub przynajmniej stosujących Szyfrowanie „in transit”.</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ korzystanie z komunikatorów niezapewniających szyfrowania danych i komunikacji typu end-to-end,</li> <li>➤ przekazywanie odbiorcom (w tym klientom) niezabezpieczonych szyfrowaniem lub hasłem danych objętych Tajemnicą zawodową).</li> </ul>
<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"> <li>➤ 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),</li> <li>➤ stosowanie oprogramowania antywirusowego rozbudowanego o moduły zapory sieciowej oraz moduł filtrowania korespondencji e-mail (np. w zakresie ochrony antyphishingowej).</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ 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).</li> </ul>

<p>2.8 3.8 3.9 4.8 7.6 7.7</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 operacyjnego i danych przed aktualizacją oprogramowania.</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ wykonywanie kopii zapasowych systemu operacyjnego zainstalowanego na komputerach i serwerach przed każdą jego aktualizacją, ale nie rzadziej niż raz na kwartał;</li> <li>➤ wykonywanie okresowych kopii zapasowych danych i aplikacji z telefonu komórkowego nie rzadziej niż raz na miesiąc;</li> <li>➤ 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;</li> <li>➤ o ile to możliwe technicznie i z uwagi na przyjęte zasady bezpieczeństwa – wykonywanie kopii zapasowych w sposób automatyczny;</li> <li>➤ oprócz szyfrowania kopii zapasowych – monitorowanie dostępu do kopii zapasowych oraz ich zabezpieczenie hasłem dostępu;</li> <li>➤ w przypadku wykonywania kopii zapasowych na zewnętrznym nośniku danych – wykonywanie kopii zapasowych na dyskach zewnętrznych HDD zabezpieczonych przed dostępem osób nieuprawnionych.</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ 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;</li> <li>➤ 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);</li> </ul>
--	---	---

		<ul style="list-style-type: none"> <li>➤ 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);</li> <li>➤ wykonywanie kopii zapasowych na pendrive'ach (pamięć USB) lub nośnikach wykorzystujących pamięć typu flash (np. dyski SSD).</li> </ul>
<p>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>	<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"> <li>➤ stosowanie środków umożliwiających utrzymanie właściwej kontroli nad sprzętem wykorzystywanym w celach zawodowych, np. hasła administratora znane jedynie Adwokatowi, zakaz wynoszenia sprzętu poza Kancelarię, itp.;</li> <li>➤ korzystanie z oprogramowania umożliwiającego zdalne zablokowanie dostępu lub usunięcie danych ze sprzętu w przypadku zgubienia lub kradzieży;</li> <li>➤ korzystanie na komputerach z wygaszaczy ekranu i automatycznego blokowania ekranu urządzenia (w tym telefonu) po krótkiej bezczynności i ponowne inicjowanie po wpisaniu hasła;</li> <li>➤ 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;</li> <li>➤ usuwanie zużytego sprzętu wraz z profesjonalnym zniszczeniem dysków twardych (lub ich zachowaniem przez kancelarię).</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ korzystanie z zewnętrznego serwisu IT w formie zdalnej bez bieżącego nadzoru;</li> <li>➤ w przypadku awarii sprzętu – przekazywanie sprzętu do serwisu (bez usunięcia</li> </ul>

		danych) bez nadzoru.
2.17 3.15	Ograniczenie lub wyłączenie działania w tle aplikacji i standardów komunikacji, które nie są wykorzystywane w sposób stały i konieczny.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ ograniczenie lub wyłączenie działania aplikacji w tle oraz standardów 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.</li> </ul>
6.7 8.7 10.2	<p>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.</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"> <li>➤ 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 Chmury Obliczeniowej);</li> <li>➤ w przypadku korzystania z usług biur serwisowanych w zakresie obsługi korespondencji (rejestracji poczty przychodzącej, skanowania poczty przychodzącej, przesyłania skanu poczty przychodzącej) – zawarcie stosownej DPA.</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ 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.</li> </ul>

<p>5.2 5.3 5.4 5.5 5.6 10.3</p>	<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 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 co najmniej WPA-2.</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><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ korzystanie wyłącznie z bezpiecznych (co najmniej zapewniających logowanie się) połączeń internetowych i transmisji danych;</li> <li>➤ 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);</li> <li>➤ w przypadku korzystania z biurowej sieci wi-fi Kancelarii – korzystanie z sieci wi-fi o standardzie szyfrowania komunikacji co najmniej WPA-2;</li> <li>➤ w przypadku korzystania z narzędzi służących do wideokonferencji – stosowanie narzędzi zapewniających szyfrowanie komunikacji end-to-end lub przynajmniej stosujących Szyfrowanie „in transit”;</li> <li>➤ korzystanie wyłącznie z zaufanych i odpowiednio zabezpieczonych przeglądarek internetowych;</li> <li>➤ regularne aktualizowanie aplikacji przeglądarek internetowych, w tym w sposób automatyczny;</li> <li>➤ korzystanie z przeglądarek po zastosowaniu wtyczek i funkcjonalności oprogramowania m.in. antywirusowego, zapory sieciowej;</li> <li>➤ aby przeglądarki internetowe korzystały (o ile to technicznie możliwe i zasadne) z rozwiązań ochrony typu endpoint<sup>5</sup>, wtyczek blokujących okienka popup<sup>6</sup>;</li> <li>➤ wyłączenie w ustawieniach przeglądarki internetowej funkcji autouzupelniania.</li> <li>➤ aby strona internetowa Kancelarii była właściwie zabezpieczona, w tym posiadała certyfikat SSL/TLS;</li> </ul>
---	--	--

<sup>5</sup> Ochrona punktów końcowych.

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

		<ul style="list-style-type: none"> <li>➤ w przypadku korzystania na stronie internetowej Kancelarii z formularzy kontaktowych zalecane jest stosownie mechanizmu CAPTCHA oraz odpowiednie zastosowanie przepisów RODO;</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ korzystanie z komunikacji internetowej pochodzącej z publicznie dostępnego wi-fi lub wi-fi znajdującego się w posiadaniu i pod nadzorem niezaufanych osób trzecich (w szczególności dotyczy do wi-fi dostępnego w biurach serwisowanych) bez jednoczesnego korzystania z zaufanego połączenia VPN;</li> <li>➤ korzystanie z komunikacji internetowej pochodzącej z wi-fi znajdującego się w posiadaniu i pod nadzorem osób trzecich (np. sieć klienta) bez jednoczesnego korzystania z zaufanego połączenia VPN;</li> <li>➤ korzystanie z usług kafejek internetowych w celach zawodowych;</li> <li>➤ 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.</li> </ul>
<p>1.3 6.11 8.8 11.6 6.12 8.11</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. Przechowywanie (retencja) danych na</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ korzystanie przede wszystkim z rozwiązań i usług informatycznych od zaufanych dostawców mających siedzibę na terytorium EOG oraz przetwarzających dane Kancelarii na terytorium EOG;</li> <li>➤ w przypadku powierzenia przetwarzania danych osobowych – zawarcie stosownej DPA;</li> <li>➤ korzystanie z rozwiązań i usług, które są regularnie aktualizowane przez dostawcę;</li> <li>➤ przed wyborem rozwiązania i usług – przeprowadzenie (w tym przy udziale</li> </ul>

	terytorium EOG.	<p>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;</p> <ul style="list-style-type: none"> <li>➤ w przypadku jakichkolwiek wątpliwości odnośnie dostawcy usług lub jakości i bezpieczeństwa świadczonych usług – rezygnację z wyboru lub korzystania z danego rozwiązania lub usługi;</li> <li>➤ korzystanie z rozwiązań i usług, których dostawcy umożliwiają wybór lokalizacji przechowywania danych.</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ 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></li> </ul>
6.8 6.9 6.10 6.12 6.13	<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><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ w przypadku korzystania przez Kancelarię ze skrzynek korespondencji e-mail w modelu SaaS konieczne jest wykorzystywanie w tym celu wyłącznie zaufanych Dostawców Usług Chmurowych;</li> <li>➤ 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);</li> <li>➤ korzystanie z usług korespondencji e-mail umożliwiających przechowywanie danych na terytorium EOG;</li> </ul>



	<p>Przechowywanie (retencja) danych na terytorium EOG.</p> <p>Przechowywanie (retencja) danych na terytorium poza EOG.</p>	<ul style="list-style-type: none"> <li>➤ okresowa archiwizacja danych (wiadomości i załączników) poza Klientem pocztowym;</li> <li>➤ prawidłowa konfiguracja narzędzi antyspamowych (wraz z właściwymi regułami) oraz stosowanie zapory sieciowej;</li> </ul> <p>W nawiązaniu również do zaleceń określonych w pkt 6.5 i 6.6:</p> <ul style="list-style-type: none"> <li>➤ 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;</li> <li>➤ zaleca się stosowanie pomiędzy Klientami pocztowymi nadawcy i adresata szyfrowania komunikacji w modelu end-to-end;</li> <li>➤ 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);</li> <li>➤ 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 haseł dostępu);</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ korzystanie z usług poczty elektronicznej w standardach innych niż biznesowe i bez zawarcia stosownej DPA, np. darmowych;</li> <li>➤ 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.</li> </ul>
--	--	---

<p>8.9 8.10 8.11</p>	<p>Korzystanie z Usług Online zapewniających możliwość kontroli logów i dostępu.</p> <p>Korzystanie z Usług Online wyłącznie w standardzie biznesowym.</p> <p>Przechowywanie (retencja) danych na terytorium EOG.</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ korzystanie z narzędzi umożliwiających monitoring/audyt logów (o ile jest to możliwe z uwagi na możliwości funkcjonalne Usługi Online);</li> <li>➤ w przypadku przetwarzania przez Kancelarię danych w Usługach Online – wykorzystywanie w tym celu wyłącznie zaufanych Dostawców Usług Chmurowych;</li> <li>➤ 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;</li> <li>➤ regularne wykonywanie dodatkowej lokalnej kopii zapasowej danych zgromadzonych w Usługach Online;</li> <li>➤ stworzenie planu ciągłości działania Usługi Online i ewentualnego jej przywracania (wraz z odzyskiwaniem danych) na wypadek awarii;</li> <li>➤ blokowanie udostępniania zasobów danych przetwarzanych w ramach Usługi Online bez dodatkowej autoryzacji.</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ przetwarzanie w Usługach Online danych objętych Tajemnicą zawodową obrońcą bez dodatkowego szyfrowania danych w sposób uniemożliwiający zapoznanie się z tymi danymi Dostawcy Usługi Online;</li> <li>➤ 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></li> </ul>
------------------------------	---	---

<p>9.3 9.4 9.5</p>	<p>Przekazywanie danych poza Kancelarię przy wykorzystaniu Usług Chmurowych w standardzie biznesowym.</p> <p>Przekazywanie danych 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><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ aby ewentualne przekazywanie przez Kancelarię danych objętych Tajemnicą zawodową poza Kancelarię (w tym klientom) nastąpiło wyłącznie przy zachowaniu właściwych standardów bezpieczeństwa i z zapewnieniem ochrony Tajemnicy zawodowej;</li> <li>➤ udostępnienia danych przy wykorzystaniu Usługi Chmurowej, której subskrybentem jest Kancelaria lub na nośnikach danych zabezpieczonych silnym hasłem dostępu;</li> <li>➤ szyfrowanie przekazywanych danych wraz z silnym hasłem dostępowym.</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ udostępnianie danych poufnych przy wykorzystaniu darmowych narzędzi i usług, niespełniających standardów biznesowych i bez zawarcia stosownej DPA;</li> <li>➤ udostępnienia danych na płytach CD/DVD-RW, na dyskach zewnętrznych lub pendrive'ach bez odpowiedniego szyfrowania.</li> </ul> <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</p>	<p>Korzystanie z usług/najmu biur serwisowanych, jeśli nie zapewniają właściwych standardów bezpieczeństwa pozwalających na utrzymanie poufności</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ aby dostęp do miejsca przechowywania dokumentów i sprzętów Kancelarii był nadzorowany i ograniczony do Personelu, z zastrzeżeniem, że klucze/karty</li> </ul>

<p>10.6 10.7</p>	<p>danych znajdujących się w posiadaniu Kancelarii, w tym informacji objętych Tajemnicą zawodową.</p> <p>Korzystanie z ogólnodostępnego sprzętu komputerowego.</p> <p>Korzystanie z ogólnodostępnego serwera.</p> <p>Skanowanie lub drukowanie na sprzęcie ogólnodostępnym.</p>	<p>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> <ul style="list-style-type: none"> <li>➤ wprowadzenie polityki czystego biurka (po zakończonej pracy wszelkie dokumenty i sprzęt przenośny powinien być przechowywany w zamykanych bezpiecznych szafach);</li> <li>➤ 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).</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ 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);</li> <li>➤ korzystanie z ogólnodostępnej sieci wi-fi, komputera lub serwera zapewnianych przez administratora biura lub wynajmującego;</li> <li>➤ skanowanie lub drukowanie dokumentów objętych Tajemnicą zawodową na ogólnodostępnym sprzęcie zapewnianym przez administratora biura lub wynajmującego.</li> </ul>
<p>1.7</p>	<p>Regularne szkolenia w zakresie wdrożonych polityk bezpieczeństwa i zasad korzystania ze sprzętu i usług.</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ aby Adwokat posiadał podstawową wiedzę z zakresu korzystania z rozwiązań informatycznych wykorzystywanych przez Kancelarię, w tym w zakresie</li> </ul>

		<p>cyberzagrożeń;</p> <ul style="list-style-type: none"> <li>➤ aby Adwokat odbywał regularne szkolenia z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa.</li> </ul>
<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"> <li>➤ korzystanie z usług zewnętrznego wsparcia informatycznego wyłącznie przy zachowaniu zasad bezpieczeństwa, w tym poufności danych znajdujących się w posiadaniu Kancelarii;</li> <li>➤ w przypadku korzystania z zewnętrznego wsparcia informatycznego w ramach, którego dostawca uzyskuje lub może uzyskać dostęp do danych osobowych – zawarcie stosownego DPA;</li> <li>➤ aby wsparcie było świadczone w biurze Kancelarii i pod nadzorem;</li> <li>➤ w przypadku korzystania ze wsparcia świadczonego w sposób zdalny nadzorowanie czynności członka personelu usługodawcy.</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ korzystanie ze wsparcia świadczonego w sposób zdalny bez stałej kontroli dostępu przez członka Personelu Kancelarii.</li> </ul>
<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"> <li>➤ aby dostęp do miejsca przechowywania dokumentów i sprzętów Kancelarii był nadzorowany i ograniczony do kręgu osób upoważnionych, 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</li> </ul>

		<p>dotyczących bezpieczeństwa biura i budynku,</p> <ul style="list-style-type: none"> <li>➤ w trakcie transportu sprzęt i nośniki danych powinny zostać w sposób właściwy zabezpieczone przed dostępem osób nieuprawnionych.</li> </ul>
1.5	Korzystanie ze sprzętu należącego do osób trzecich, w szczególności przy dostępie do informacji objętych Tajemnicą zawodową.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ korzystanie wyłącznie ze sprzętu służbowego Kancelarii w celach zawodowych celem zminimalizowania kręgu osób, które mogą mieć dostęp do Tajemnicy zawodowej.</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ korzystanie ze sprzętu należącego do osób trzecich, skanowania lub drukowania na takim sprzęcie, a w szczególności przy dostępie do informacji objętych Tajemnicą zawodową;</li> <li>➤ skanowanie lub drukowanie poza biurem na sprzęcie należącym do osób trzecich (w tym w kafejkach internetowych i biurach serwisowanych).</li> </ul>
1.8	Wykupienie ubezpieczenia w zakresie odpowiedzialności dotyczącej cyberbezpieczeństwa i RODO.	<p><u>Zalecane opcjonalnie jest:</u></p> <ul style="list-style-type: none"> <li>➤ wykupienie przez Kancelarię stosownego ubezpieczenia w zakresie odpowiedzialności Kancelarii za szkody spowodowane przez Incydenty.</li> </ul>

ROZDZIAŁ II  
ZALECENIA DODATKOWE – KANCELARIE MAŁE, ŚREDNIE I DUŻE

NUMER ZALECENIA	CZEGO DOTYCZY?	WYJAŚNIENIA
1.1	Korzystanie wyłącznie z licencjonowanego i aktualnego oprogramowania przeznaczonego do komercyjnego zastosowania.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ 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).</li> </ul>
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.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ 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.</li> </ul>
1.6	Okresowy przegląd cyberzagrożeń i dostosowanie stosownych środków technicznych i organizacyjnych przy uwzględnieniu istniejących i potencjalnych ryzyk.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ przeprowadzanie okresowych przeglądów i audytów wewnętrznych wymagań dla wykorzystywanych rozwiązań i sprzętu, z uwagi na zmieniającą się technikę informatyczną;</li> <li>➤ dostosowanie stosowanych środków technicznych i organizacyjnych przy uwzględnieniu istniejących i potencjalnych ryzyk dla bezpieczeństwa danych przetwarzanych przez Kancelarię;</li> <li>➤ stosowanie modelu PDCA (Plan-Do-Check-Act), podejścia Privacy by Design i</li> </ul>

		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"> <li>➤ 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,</li> <li>➤ aby decyzja o okresowej zmianie haseł lub jej częstotliwość uwzględniona była we wdrożonych procedurach bezpieczeństwa oraz systemie zarządzania bezpieczeństwem informacji.</li> </ul>
13.1	Stosowanie polityki zarządzania konfiguracją, dostępem oraz monitorowaniem dostępu i sieci.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ w przypadku Kancelarii małych (posiadających wykwalifikowane stałe wsparcie informatyczne), średnich i dużych – wdrożenie polityki zarządzania dostępami 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),</li> <li>➤ aby przydzielane użytkownikom loginy były zindywidualizowane, tj. przypisane tylko do jednego użytkownika i w sposób zapewniający jego identyfikację,</li> <li>➤ 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,</li> <li>➤ w przypadku Kancelarii małych, średnich i dużych – wprowadzenie klasyfikacji uprawnień i kategorii użytkowników,</li> <li>➤ w przypadku Kancelarii małych (posiadających wykwalifikowane stałe wsparcie informatyczne), średnich i dużych – prowadzenie monitorowania sieci (w tym ruchu</li> </ul>



		<p>sieciowego i urządzeń sieciowych) wraz z automatycznym powiadomieniem o wykrytych zagrożeniach,</p> <ul style="list-style-type: none"> <li>➤ w przypadku Kancelarii dużych – rozważenie korzystania z systemów detekcji anomalii IDPS (Intrusion Detection / Prevention System) oraz SIEM (Security Incident and Event Management),</li> <li>➤ w przypadku Kancelarii średnich i dużych – rozważenie wprowadzenia segmentacji sieci wewnętrznej poprzez wydzielenie sieci VLAN (virtual local area network).</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ 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).</li> </ul> <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>
13.2	Wdrożenie w Kancelarii norm ISO z rodziny ISO/IEC 27000.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ 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),</li> </ul>

		<p>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).</p> <p>Uzyskanie certyfikatu zgodności z normami ISO nie jest konieczne. Wdrożenie ww. norm w Kancelarii małej jest zalecane opcjonalnie.</p>
13.3	<p>Wdrożenie wewnętrznych polityk bezpieczeństwa w zakresie przetwarzania w Kancelarii informacji (w szczególności dotyczącej retencji danych), w tym danych objętych Tajemnicą zawodową.</p>	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ wdrożenie wewnętrznej polityki bezpieczeństwa przetwarzanych informacji, w szczególności zawierającej wytyczne dotyczące przetwarzania danych. W przypadku Kancelarii małych jest to zalecenie opcjonalne.</li> </ul> <p>W przypadku wdrożenia polityki bezpieczeństwa przetwarzanych informacji Kancelaria powinna zidentyfikować kluczowe zasoby informacji, w szczególności informacje i dokumenty klientów, kluczowe usługi i rejestry/zbiory, które mają krytyczne znaczenie dla jego działalności. Ponadto, polityka powinna zawierać przy tym m.in.:</p> <ul style="list-style-type: none"> <li>a) identyfikację potencjalnych zagrożeń i Incydentów (wraz z prawdopodobieństwem wystąpienia) oraz rozważeniem możliwych reakcji/środków;</li> <li>b) identyfikację procesów realizowanych w organizacji Kancelarii;</li> <li>c) politykę zarządzania siecią, sprzętem, usługami i uprawnieniami;</li> <li>d) stosowną dokumentację z zakresu ochrony danych osobowych (jeśli jest wymagana).</li> </ul>

13.4	Wdrożenie planu ciągłości działania istotnych elementów infrastruktury (usług) informatycznej Kancelarii i odzyskiwania danych (data recovery).	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ wdrożenie planu ciągłości działania istotnych elementów infrastruktury (usług) informatycznej Kancelarii i odzyskiwania danych (data recovery). W przypadku Kancelarii małych jest to zalecenie opcjonalne.</li> </ul>
13.5	Regularne szkolenia Personelu w zakresie wdrożonych polityk bezpieczeństwa i zasad korzystania ze sprzętu i usług.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ przeprowadzanie regularnych szkoleń Personelu z zakresu stosowanych w Kancelarii polityk i procedur, w szczególności dotyczących bezpieczeństwa informacji i cyberbezpieczeństwa.</li> </ul>
13.6	Powierzenie administrowania i nadzoru nad infrastrukturą informatyczną Kancelarii osobie pełniącej funkcję Administratora Systemu Informatycznego (ASI).	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ powierzenie administrowania i nadzoru nad infrastrukturą informatyczną Kancelarii osobie pełniącej funkcję Administratora Systemu Informatycznego (ASI) na podstawie odpowiedniej umowy;</li> <li>➤ w przypadku Kancelarii dużych – aby funkcję ASI pełnił wykwalifikowany członek Personelu.</li> </ul> <p>W przypadku Kancelarii małych jest to zalecenie opcjonalne.</p>
13.7	Posiadanie ubezpieczenia w zakresie odpowiedzialności dotyczącej cyberbezpieczeństwa i RODO.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ wykupienie przez Kancelarię stosownego ubezpieczenia w zakresie odpowiedzialności Kancelarii za szkody spowodowane przez Incydenty.</li> </ul>
13.8	Aktualizacja oprogramowania przy wykorzystaniu środowiska testowego, w	<p><u>Zalecane jest:</u></p>

	<p>celu weryfikacji wpływu aktualizacji na działanie tych systemów i ewentualnego wykrycia podatności.</p>	<ul style="list-style-type: none"> <li>➤ 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.</li> </ul> <p>W przypadku Kancelarii małych i średnich jest to zalecenie opcjonalne.</p>
<p>14.1 14.2 14.3 14.4 15.1 15.2 15.3 16.1</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><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ stosowanie aplikacji do administracyjnego zarządzania urządzeniami (MDM);</li> <li>➤ stosowanie Hasła administratora z pełnym dostępem do zasobów i ustawień systemu, deponowane w bezpiecznej kopercie w szafie pancerniej. Pozwoli to zabezpieczyć dostęp do zasobów Kancelarii w przypadku zaistnienia Incydentu;</li> <li>➤ w przypadku serwerów – stosowanie zasilania UPS;</li> <li>➤ w przypadku serwerów kolokowanych u podmiotów trzecich zalecane jest stosowanie redundancji łączy i narzędzi sieciowych;</li> <li>➤ korzystanie przez Personel w celach zawodowych wyłącznie ze sprzętu służbowego;</li> <li>➤ wdrożenie polityki bezpieczeństwa (w szczególności w przypadku eksploatacji serwera lokalnego);</li> <li>➤ 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).</li> </ul> <p><u>Niezalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ aby serwery własne, serwery kolokowane i hostowane, a także serwery</li> </ul>

		<p>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);</p> <ul style="list-style-type: none"> <li>➤ stosowanie polityki korzystania przez Personel w celach zawodowych z prywatnego sprzętu (tzw. BYOD);</li> <li>➤ korzystanie z zewnętrznego serwisu IT w formie zdalnej bez bieżącego nadzoru członka Personelu;</li> <li>➤ w przypadku awarii sprzętu – przekazywanie sprzętu do serwisu (bez usunięcia danych) bez nadzoru członka Personelu.</li> </ul>
17.1	Korzystanie z własnego serwera pocztowego.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ 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;</li> <li>➤ blokowanie możliwości (bez autoryzacji) przesyłania przez członka Personelu za pośrednictwem korespondencji e-mail większych paczek danych;</li> <li>➤ wprowadzenie możliwości dokonywania przez Personel zgłoszeń podejrzanych wiadomości e-mail obejmowanych automatycznie kwarantanną (przed ich analizą przez administratora).</li> </ul>
18.1 19.1 20.1	Wdrożenie polityki wydawania danych uprawnionym organom w przypadkach określonych przepisami prawa.	<p><u>Zalecane jest:</u></p> <ul style="list-style-type: none"> <li>➤ wdrożenie polityki dostępu i wydawania danych uprawnionym organom w przypadkach określonych przepisami praw; w szczególności zawierających procedurę zapewnienia zachowania Tajemnicy zawodowej.</li> </ul>

21.1	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"><li>➤ w przypadku Kancelarii średnich i dużych – korzystanie z usług podmiotu posiadającego zweryfikowaną wiedzę z zakresu rozwiązań sieciowych i ISO z rodziny ISO/IEC 27000.</li></ul> <p>W przypadku Kancelarii małych jest to zalecenie opcjonalne.</p>
------	---	--