

Polityka Ochrony Danych Osobowych
w Kancelarii Notarialnej
prowadzonej przez GRZEGORZA MROWIŃSKIEGO
Notariusza w Białogardzie

ADMINISTRATOR DANYCH OSOBOWYCH: NOTARIUSZ Grzegorz Mrowiński

INSPEKTOR OCHRONY DANYCH: Nie został wyznaczony

ADMINISTRATOR SYSTEMU INFORMATYCZNEGO: Nie został wyznaczony

I. POSTANOWIENIA OGÓLNE

§ 1.

Wprowadzenie

1. Niniejsza Polityka Ochrony Danych Osobowych (dalej PODO) jest nadrzędnym obowiązującym w kancelarii dokumentem określającym strategię ochrony danych, plan działań mający umożliwić osiągnięcie celu, jakim jest skuteczna ochrona danych, w tym reguły, cele oraz zasady ochrony danych osobowych stosowane przez Notariusza, zwanego dalej Administratorem.
2. Dokument stanowi jeden ze środków technicznych i organizacyjnych, którego celem jest wykazanie zgodności realizowanych czynności przetwarzania z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej RODO).
3. Do przestrzegania niniejszej polityki zobowiązany jest Administrator oraz wszyscy pracownicy kancelarii a także osoby, które przetwarzają dane osobowe na podstawie upoważnienia Administratora, bez względu na formę realizacji z Administratorem.
4. W przypadku współpracy z podmiotem trzecim obejmującej przetwarzanie danych osobowych na zlecenie Administratora, Administrator zapewnia, by podmiot ten zobowiązał się do zapewnienia odpowiedniego poziomu ochrony danych osobowych z uwzględnieniem postanowień Polityki Ochrony Danych Osobowych.
5. Zagwarantowanie właściwej ochrony danym osobowym przetwarzanych w kancelarii stanowi istotny element strategii działania w zakresie zapewnienia bezpieczeństwa danych osobowych, w części objętych tajemnicą prawnie chronioną wynikającą z charakteru działań wykonywanych przez Notariusza.
6. Notariusz jako Administrator zapewnia przestrzeganie wymagań regulacyjnych wynikających z Unijnego rozporządzenia (dalej RODO), ustawy z dnia 14 lutego 1991 r. Prawo o notariacie (t.j. Dz. U. z 2024 r. poz. 1001) oraz innych aktów normatywnych dotyczących przetwarzania danych osobowych.
7. Dane osobowe sygnalisty, podlegają ochronie z uwzględnieniem przepisów ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz. U. poz. 928) oraz art. 53 i 53a ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2023 r. poz. 1124 z późn. zm.).

§ 2.

Podstawowe cele PODO

Dokument niniejszy stanowi fundament systemu ochrony danych osobowych funkcjonujący w kancelarii, który określa podstawowe cele ochrony danych osobowych w środowisku przetwarzania Administratora. Do celów tych należy:

- 1) zapewnienie ochrony przed nieupoważnionym dostępem do danych

2) zapewnienie poufności, dostępności i integralności danych osobowych przetwarzanych w kancelarii

3) zapewnienie ciągłości realizacji procesów przetwarzania dla utrzymania dostępności i integralności informacji

4) zapewnienie monitorowania zgodności działania kancelarii z zasadami ochrony danych osobowych oraz innymi regulacjami prawnymi

5) zapewnienie realizacji praw podmiotów, których dane osobowe są przetwarzane

6). zapewnienie prawidłowego powierzenia i udostępnienia danych osobowych podmiotom trzecim

7) zapewnienie dokumentowania naruszeń ochrony danych osobowych

8) zapewnienie świadomości pracowników w zakresie prawidłowego przetwarzania danych osobowych

§ 3.

Określenia i użyte skróty

Użyte w Polityce określenia oznaczają:

1. Administrator Danych Osobowych, dalej jako Administrator – Notariusz Grzegorz Mrowiński

2. Polityka - Polityka ochrony danych.

3. 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 (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119).

4. dane osobowe - dane osobowe w rozumieniu art. 4 pkt 1 RODO.

5. pracownik - osoba zatrudniona w kancelarii oraz świadcząca na rzecz kancelarii jakąkolwiek pracę za wynagrodzeniem albo bez wynagrodzenia, bez względu na formę relacji z Administratorem, w tym stażysta, wolontariusz, praktykant, aplikant, osoba świadcząca usługi na podstawie umów cywilnoprawnych, zastępca notariusza, bez względu na sposób jego wyznaczenia (w tym zastępca notarialny, inny notariusz oraz emerytowany notariusz), jak również członek rodziny Administratora, wykonujący pracę jako osoba współpracująca w rozumieniu ustawy o systemie ubezpieczeń społecznych albo świadcząca okazijną pomoc Administratorowi.

6. osoba nieupoważniona - osoba nieposiadająca upoważnienia do przetwarzania danych osobowych w zakresie niezbędnym do wykonania czynności;

7. osoba upoważniona - osoba przetwarzająca dane osobowe, w tym również za pomocą systemu informatycznego lub sieci teleinformatycznej, w ramach wykonywanych zadań służbowych w zakresie określonym w upoważnieniu;

8. hasło - ciąg znaków literowych, cyfrowych lub innych znanych jedynie osobie uprawnionej do pracy w systemie informatycznym;

9. identyfikator - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

II. ZASADY ORGANIZACYJNE

§ 4.

Organizacja systemu bezpieczeństwa przetwarzania danych osobowych

1. Administrator uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, podejmuje odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2. Administrator uznał wdrożenie polityki ochrony danych za proporcjonalne w stosunku do czynności przetwarzania.

3. Zważywszy, że:

a) Administrator nie jest organem lub podmiotem publicznym,

b) główna działalność administratora nie polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,

c) główna działalność administratora nie polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 RODO, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10 RODO,

a nadto biorąc pod uwagę:

- zakres przetwarzanych danych,

- szczególną ochronę danych wynikającą z tajemnicy notarialnej,

- kwestie organizacyjne, w tym: brak rozbudowanej struktury organizacyjnej Kancelarii, ilość zatrudnionych osób, przetwarzanie danych osobowych w ilości, zakresie i przy użyciu środków, adekwatnych do podmiotów przetwarzających te dane,

Administrator podjął decyzję o niewyznaczeniu Inspektora Ochrony Danych Osobowych, Administratora Bezpieczeństwa Systemów Informatycznych i Administratora Systemów Informatycznych.

4. Do momentu wyznaczenia Inspektora Ochrony Danych Osobowych, Administratora Bezpieczeństwa Systemów Informatycznych i Administratora Systemów Informatycznych, obowiązki tych osób, pełni Administrator.

5. Za prawidłowość przetwarzania danych osobowych i ich ochronę w Kancelarii odpowiada Administrator i pracownicy.

6. Administrator:

1) realizuje zadania wynikające z Polityki;

2) wdraża oraz nadzoruje przestrzeganie Polityki;

3) organizuje i nadzoruje funkcjonowanie systemu zabezpieczeń danych osobowych;

- 4) realizuje obowiązki, o których mowa w art. 14-21 RODO;
- 5) regularnie dokonuje przeglądu upoważnień do przetwarzania danych osobowych w celu zapewnienia ich aktualności;
- 6) podejmuje decyzje dotyczące sposobu przetwarzania danych osobowych;
- 7) zawiera umowy dotyczące przetwarzania danych osobowych, w tym powierzenia przetwarzania danych osobowych.

7. Pracownicy:

- 1) przestrzegają przepisów RODO, przepisów regulujących ochronę danych osobowych oraz postanowienia Polityki;
- 2) składają oświadczenia o:
 - a) zachowaniu tajemnicy służbowej, w tym zachowaniu w tajemnicy danych osobowych,
 - b) zapoznaniu się z przepisami RODO, regulującymi ochronę danych osobowych oraz Polityką;
- 3) przetwarzają dane osobowe zgodnie z celem, dla którego zostały one zebrane;
- 4) zgłaszają Administratorowi zdarzenia związane z bezpieczeństwem danych osobowych.

§ 5.

Bezpieczeństwo informacji

1. Organizacja systemu ochrony informacji w kancelarii ma na celu zapewnić bezpieczeństwo informacji przed ich utratą, niekontrolowaną zmianą lub ujawnieniem treści zastrzeżonych, niezależnie od miejsca oraz sposobu jej przetwarzania, przesyłania i przechowywania.
2. Proces ten realizowany jest w oparciu o następujące założenia:
 - 1) informacja dostępna jest wyłącznie dla osób uprawnionych, posiadających odpowiednie prawa dostępu do informacji (poufność)
 - 2) informacja jest dokładna, kompletna i nie podatna na niekontrolowane lub nieautoryzowane zmiany (integralność)
 - 3) informacja jest dostępna dla osoby upoważnionej zawsze kiedy tego potrzebuje (dostępność)
 - 4) każde działanie jest przypisane do osoby fizycznej lub procesu oraz umiejscowione w czasie (rozliczalność)
 - 5) zawartość informacji oraz jej pochodzenie jest takie jak deklarowano (autentyczność)
 - 6) niemożliwe jest zanegowanie uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie (niezaprzeczalność)

§ 6.

Upoważnienie

1. Udzielając dostępu do przetwarzania danych osobowych stosuje się zasadę wiedzy koniecznej polegającą na dostępie do danych niezbędnych do wykonywania służbowych obowiązków.
2. Dostęp do danych osobowych mają osoby uprawnione na podstawie imiennego pisemnego upoważnienia do przetwarzania danych osobowych, z zastrzeżeniem ust. 2.

3. W szczególnie uzasadnionym przypadku (np. wyznaczenie zastępcy notariusza), do czasu uzyskania pisemnego upoważnienia do przetwarzania danych osobowych, o którym mowa w ust. 4, dostęp do danych osobowych mogą mieć osoby, którym Administrator udzielił ustnego upoważnienia.

4. Upoważnienie do przetwarzania danych osobowych jest udzielane przez Administratora bądź osobę przez niego wskazaną, po zapoznaniu upoważnianego z Polityką oraz odebraniem od niego oświadczenia, o którym mowa w § 4 ust. 7 pkt 2 Polityki.

5. Upoważnienie do przetwarzania danych osobowych jest jednocześnie upoważnieniem do przetwarzania danych osobowych w systemie informatycznym, chyba, że z treści tego upoważnienia wynika inaczej. Administrator dokonując analizy struktury personalnej kancelarii ustalił, że każdy pracownik posiadający upoważnienie do przetwarzania danych osobowych, będzie przetwarzał je w systemie informatycznym kancelarii, wobec czego wprowadzenie odrębnych upoważnień nie jest celowe.

6. Po udzieleniu upoważnienia Administrator tworzy indywidualne konto użytkownika oraz nadaje identyfikator i hasło. Hasło do systemu informatycznego jest przekazywane przy uruchomieniu konta bezpośrednio użytkownikowi a użytkownik informowany jest o zasadach posługiwania się loginem i hasłem oraz ich zmiany.

7. Upoważnienie traci moc w przypadku:

1) rozwiązania lub wygaśnięcia umowy o pracę (bądź innego stosunku służbowego łączącego pracownika z Administratorem);

2) wygaśnięcia upoważnienia wydanego na czas określony.

3) cofnięcia przez Administratora upoważnienia do przetwarzania danych osobowych.

8. W przypadku utraty mocy upoważnienia, Administrator niezwłocznie podejmuje czynności, w celu odebrania dostępu do zasobów informatycznych.

§ 7.

Podstawowe zasady przetwarzania danych osobowych

1. Przetwarzanie danych osobowych w kancelarii oparte zostało o 4 filary:

I. Zgodność z prawem:

1) legalność - dane osobowe przetwarzane są wyłącznie na podstawie zgody osoby, której dotyczą lub na innej uzasadnionej podstawie przewidzianej prawem

2) rzetelność - podmiot danych posiada informację, że jego dane osobowe są przetwarzane przez Administratora

3) przejrzystość - wszelkie informacje kierowane przez Administratora do osoby, której dane dotyczą są zwięzłe, łatwo dostępne i zrozumiałe oraz formułowane jasnym i prostym językiem

4) ograniczony cel przetwarzania - dane osobowe przetwarzane są tylko w konkretnych i wyraźnych celach

5) minimalizacji danych - pozyskiwane są tylko takie dane osobowe, które są konieczne do osiągnięcia zamierzonego celu

6) prawidłowość danych - dane osobowe są kompletne, zgodne z prawdą, a w razie stwierdzenia ich nieprawdziwości lub niekompletności uaktualniane

7) ograniczenia przechowywania danych - dane osobowe są przechowywane przez okres nie dłuższy, niż jest to konieczne dla uzyskania celów, dla których były one przetwarzane

8) integralność i poufność danych osobowych - dane osobowe są przetwarzane w sposób zapewniający ich ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem danych oraz przypadkową ich utratą, zniszczeniem lub uszkodzeniem.

II. Bezpieczeństwo danych - Administrator zapewnia odpowiedni poziom bezpieczeństwa danych poprzez wdrożenie takich środków organizacyjnych i technicznych, które są adekwatne do ryzyka wystąpienia naruszeń bezpieczeństwa przetwarzanych danych. Skuteczność środków organizacyjnych i technicznych mających zapewnić bezpieczeństwo przetwarzania jest regularnie testowana, mierzona i oceniana.

III. Prawa podmiotów danych - Administrator umożliwia realizację praw osób, których dane osobowe są przetwarzane w kancelarii

IV. Rozliczalność - poprzez odpowiednie środki Administrator utrwała i przechowuje informacje pozwalające na wykazanie zgodności podjętych przez Administratora działań zgodnie z przepisami prawa.

2. Administrator opracowuje i aktualizuje Rejestr czynności przetwarzania danych osobowych.

3. Dane osobowe są przetwarzane w Kancelarii tylko i wyłącznie na zasadach określonych w RODO.

4. Dane osobowe w Kancelarii przetwarzane są wyłącznie w przypadkach, gdy jest to niezbędne do:

1) wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

2) wypełnienia obowiązku prawnego ciążącego na administratorze;

3) ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

4) wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

5. Administrator oraz pracownicy, którzy pozyskują dane osobowe informują osoby, których te dane dotyczą o:

1) adresie Kancelarii;

2) danych Administratora;

3) celach przetwarzania danych osobowych oraz podstawie prawnej przetwarzania;

4) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

5) gdy ma to zastosowanie - zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;

6) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;

7) prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

8) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO - prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

9) prawie wniesienia skargi do organu nadzorczego;

10) tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

11) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;

12) celu innym niż cel, w którym dane osobowe zostały zebrane chyba, że przepisy szczególne stanowią inaczej.

6. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, osobę, której dotyczą te dane, należy poinformować ponadto o źródle danych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych.

7. Zasady określone w ust. 1 i 2 nie mają zastosowania w przypadku, gdy:

1) przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania;

2) osoba, której dane dotyczą, posiada informacje określone w ust. 1 lub 2.

8. W przypadku wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem RODO lub są zbędne do realizacji celu, dla którego je zebrano, Administrator jest obowiązany w szczególności do ich uzupełnienia, uaktualnienia, sprostowania, usunięcia lub ograniczenia przetwarzania, chyba, że odpowiednie przepisy tego zabraniają.

9. Dane osobowe przetwarzane w Kancelarii są przechowywane przez okres wynikający z obowiązujących przepisów.

10. Dane osobowe kandydatów do pracy w Kancelarii zawarte w ofertach zgłaszanych w odpowiedzi na ogłoszenia o naborze na wolne stanowiska pracy oraz aplikację, staż, praktykę lub wolontariat mogą być przechowywane maksymalnie 3 miesiące od dnia zakończenia rekrutacji.

11. Po upływie okresu przechowywania danych, dokumenty zawierające dane osobowe są niszczone, chyba, że inny sposób postępowania z nimi przewidują odpowiednie przepisy.

§ 8

Zarządzanie ryzykiem i ocena skutków

1. Ocena ryzyka przeprowadzana przez Administratora polega na szczegółowej analizie prowadzonych procesów przetwarzania danych i dokonania oceny na jakie przetwarzanie danych w konkretnym przypadku jest narażone. W procesie tym dokonywana jest ocena na podstawie czynników prawdopodobieństwa oraz skutku zdarzenia mającego negatywny wpływ na bezpieczeństwo danych osobowych.
2. Administrator przeprowadza również ocenę skutków (DPIA) procesów przetwarzania o ile dany proces wymaga jej przeprowadzenia.

§ 9

Udostępnianie i powierzenia danych osobowych

1. Administrator korzysta wyłącznie z usług takich podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą.
2. Powierzenie przetwarzania danych osobowych podmiotom przetwarzającym następuje w drodze umowy zawartej na piśmie lub przy pomocy innego instrumentu prawnego.

§ 10

Naruszenie lub naruszenia ochrony danych

1. Przez naruszenie ochrony danych rozumie się naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
2. W każdym wypadku Administrator bada zaistniałe naruszenie i wdraża stosowne organizacyjne i techniczne środki naprawcze oraz dokonuje wszelkich starań, aby pracownicy i współpracownicy mieli wiedzę niezbędną do prawidłowego rozpoznawania sytuacji mogących stanowić Naruszenie ochrony danych osobowych.

§ 11

Realizacja praw podmiotów

1. Administrator zapewnia realizację praw osób fizycznych określonych w rozdziale III RODO. Komunikacja z podmiotem danych poprzez wdrożenie odpowiednich środków odbywać się powinna w zwięzłej, przejrzystej i łatwo dostępnej formie.
2. Ze względu na wyjątkowy charakter czynności wykonywanych przez Notariusza realizacja praw podmiotów w danym przypadku może zostać ograniczona i realizowana na zasadach określonych w ustawie Prawo o notariacie (art. 78b) oraz ustawie o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (art. 53-54).

III. ŚRODKI OCHRONY DANYCH

§ 12

Techniczne środki ochrony danych osobowych

1. Dane osobowe mogą być przetwarzane w Kancelarii wyłącznie w pomieszczeniach odpowiednio zabezpieczonych przed nieuprawnionym dostępem, zaś wyjątkowo w pomieszczeniach ogólnodostępnych, w sposób zapewniający poufność tych danych.
2. Przetwarzania danych osobowych poza kancelarią powinno następować wyjątkowo, w szczególności jeśli wymaga tego charakter czynności przetwarzania danych osobowych, np. czynność wyjazdowa albo przekazanie wypisów aktów notarialnych sądom i urzędowi. Dane osobowe powinny być wówczas należycie chronione.
3. Przetwarzanie danych osobowych znajdujących się na nośnikach mobilnych oraz sprzęcie przenośnym, dopuszczalne jest jedynie na sprzęcie służbowym, zabezpieczonym przed nieuprawnionym dostępem do tych danych.
4. Administrator zapewnia stosowną ochronę zasobów teleinformatycznych kancelarii poprzez zastosowanie odpowiedniej wiedzy i środków, co stanowi nadrzędny cel w zapewnieniu bezpieczeństwa aktywów teleinformatycznych przez Administratora.
5. Poprzez zapewnienie bezpieczeństwa teleinformatycznego w kancelarii rozumie się zidentyfikowanie zagrożeń obszaru przetwarzania w systemach teleinformatycznych, a do odpowiadających im podatności zastosowanie odpowiednich zabezpieczeń technicznych i organizacyjnych.
6. W ochronie systemu teleinformatycznego kancelarii uwzględnia się takie elementy jak:
 - a. zarządzanie aktywami
 - b. kontrole dostępu
 - c. środki ochrony kryptograficznej
 - d. bezpieczeństwo fizyczne i środowiskowe oraz bezpieczeństwo eksploatacji
 - e. bezpieczeństwo komunikacji
 - f. pozyskiwanie, rozwój i utrzymywanie systemów teleinformatycznych
 - g. relacje z dostawcami
 - h. zarządzanie incydentami
 - i. zarządzanie ciągłością działania
 - j. nadzór nad systemami teleinformatycznymi (testowanie, monitorowanie)

§ 13

Informatyczne środki ochrony danych osobowych

1. Hasło do systemu informatycznego nie może być powszechnie używanymi słowami.
2. Użytkownik systemu informatycznego jest obowiązany zachować hasło w poufności, nawet po utracie przez nie ważności oraz do niezwłocznej zmiany tego hasła, gdy zostało ono ujawnione.
3. Zabronione jest zapisywanie hasła w sposób jawny oraz przekazywanie go innym osobom.

4. Hasło jest zmieniane w sposób automatyczny. W przypadku braku wymuszenia zmiany hasła przez system informatyczny, użytkownik systemu informatycznego jest obowiązany zmieniać hasło samodzielnie w terminie nie dłuższym niż co 60 dni.
5. Hasło składa się z co najmniej 8 znaków, w tym dużych i małych liter oraz z cyfr lub znaków specjalnych. W hasle nie może być zawarty w szczególności: identyfikator, imię lub nazwisko, stanowisko, symbol lub nazwa użytkownika systemu informatycznego, przewidywalna sekwencja znaków, w tym "QWERTY", "12345678".
6. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer/nazwa miesiąca lub inny możliwy do odgadnięcia klucz.
7. Dane osobowe znajdujące się na nośnikach służących do zapisu i przechowywania informacji, np. zewnętrznych dyskach twardych, pamięciach przenośnych flash, płytach wielokrotnego zapisu, przed udostępnieniem osobom upoważnionym należy zabezpieczyć nadając hasło w programie 7-zip lub w innym równoważnym programie i zapisać w formacie zgodnym z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247). Dane mogą zostać zapisane również w innym programie, jeżeli nie są kierowane do podmiotów administracji publicznej a odbiorca wyraził zgodę na odbiór danych w uzgodnionym formacie.
8. Dane osobowe udostępniane przy pomocy poczty elektronicznej należy przed wysłaniem zabezpieczyć nadając hasło w programie 7-zip lub w innym równoważnym programie i zapisać w formacie zgodnym z Krajowymi Ramami Interoperacyjności (np. zip). Zabezpieczenie może nastąpić również poprzez zabezpieczenie hasłem dostępu do plików zawierających dane, typu .pdf, .doc, .xls, zip, .xml). Dane mogą zostać zapisane również w innym programie, jeżeli nie są kierowane do podmiotów administracji publicznej a odbiorca wyraził zgodę na odbiór danych w uzgodnionym formacie. Powyższe nie dotyczy danych osobowych przekazywanych w Elektronicznym Portalu Obsługi Notariuszy, z uwagi na wielostopniową weryfikację uprawnień dostępowych do tego systemu i autentykację, przy użyciu podpisu elektronicznego.
9. Hasła do zabezpieczonych plików należy przekazać odbiorcy pliku ustnie lub innym kanałem komunikacyjnym niż zabezpieczony plik. W żadnym wypadku nie jest dopuszczalne przesyłanie zabezpieczonego pliku wraz z hasłem.
11. Użytkownik systemu informatycznego loguje się do systemu informatycznego przetwarzającego dane osobowe z użyciem identyfikatora i hasła.
12. Użytkownik systemu informatycznego jest obowiązany powiadomić administratora o próbach logowania się do systemu informatycznego osoby nieupoważnionej, jeżeli system to sygnalizuje,

w szczególności w przypadku zablokowania dostępu do programów lub karty kryptograficznej w wyniku kilkukrotnego wprowadzenia błędnego hasła.

13. Użytkownik systemu informatycznego jest obowiązany do stosowania polityki czystego ekranu, polegającej na uniemożliwieniu osobom niepowołanym - osobom, które nie posiadają upoważnienia do przetwarzania danych osobowych - wglądu do danych osobowych wyświetlanych na monitorach komputerowych.

14. Opuszczając na określony czas stanowisko pracy, użytkownik systemu informatycznego jest obowiązany wywołać blokowany hasłem wygaszacz ekranu, zablokować system lub wylogować się z systemu.

15. Po zakończeniu pracy, użytkownik systemu informatycznego jest obowiązany wylogować się z systemu informatycznego, ewentualnie wyłączyć sprzęt komputerowy oraz stosować politykę czystego biurka dla dokumentów - wydruków z systemu informatycznego oraz nośników - zawierających dane z systemu informatycznego.

§ 14

Procedury tworzenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania

1. W Kancelarii mogą być tworzone kopie bezpieczeństwa wszystkich systemów, w których przetwarzane są dane osobowe wraz ze środowiskiem.

2. Administrator podejmuje decyzję o wykonywaniu kopii, biorąc pod uwagę zasób systemów, użytkowników i urządzeń kancelarii, przygotowuje i aktualizuje plan wykonywania kopii zapasowych. Częstotliwość oraz zakres wykonywanych kopii zapasowych ustalany jest adekwatnie do celów Kancelarii i znaczenia archiwizowanych danych dla Kancelarii.

3. Kopie całościowe wykonywane są z częstotliwością nie mniejszą niż 90-dniową.

4. Kopie przyrostowe mogą być sporządzane na streamerze, serwerze (mirror), pamięci przenośnej flash lub dysku wymiennym.

5. W przypadku, gdy kopia zapasowa jest wykonywana po raz pierwszy, wymagane jest wykonanie kopii pełnej (całościowej).

6. Każdą kopię należy czytelnie opisać co do zawartości i daty sporządzenia.

7. Dostęp do kopii ma Administrator oraz pracownicy wyznaczeni przez Administratora.

8. Administrator jest obowiązany do sporządzenia kopii oraz weryfikacji ich poprawności i możliwości ponownego odtworzenia. Administrator może powierzyć to zadanie wyznaczonemu pracownikowi lub zlecić je zewnętrznej obsłudze informatycznej, posiadającej odpowiednie upoważnienie.

9. Niszczenie kopii odbywa się poprzez trwałe fizyczne zniszczenie nośnika lub nieodwracalne usunięcie danych z nośnika z użyciem specjalnego oprogramowania.

10. Administrator, przed wykonaniem kopii zapasowej, o ile ma to zastosowanie, testuje nośniki, na których zapisane będą dane osobowe, pod względem poprawności ich działania.

11. Do typowych nośników informacji należą: pamięci przenośne flash, przenośne twarde dyski, płyty z możliwością zapisu danych, przenośne komputery osobiste.
12. Użytkownicy systemu informatycznego są obowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników po ustaniu celu ich przetwarzania na nośnikach informacji.
13. Nośniki należy przechowywać w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczyć je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).
14. Zabrania się przekazywania nośników z nieusuniętymi danymi osobowymi podmiotom lub osobom zewnętrznym (kontrola dostępu osób reprezentujących podmioty zewnętrzne do elektronicznych nośników informacji jest określana w umowie z tymi podmiotami).
15. Zabrania się pozostawiania nośników dostępnych dla osób nieupoważnionych (polityka czystego biurka).
16. Nośniki używane w kancelarii powinny być przechowywane zgodnie z zaleceniami producenta.
17. W przypadku ryzyka pogorszenia się stanu nośnika informacji (w tym nośników z kopiami zapasowymi), na którym przechowywane są istotne, wciąż wykorzystywane dane, Administrator dokonuje przeniesienia danych na nowy nośnik.
18. W przypadku konieczności transportu nośników informacji (w tym kopii zapasowych), należy korzystać z własnego transportu, nadzorowanego przez administratora lub pracowników kancelarii oraz bezpiecznie pakować sprzęt i nośniki, zgodnie z zaleceniami producenta w celu zapewnienia ochrony przed wpływem czynników środowiskowych.
19. Kopie zapasowe, w przypadku, gdy wykonywane są na odrębnych nośnikach, przechowywane są, o ile jest to możliwe, w innym pomieszczeniu niż serwerownia, w sejfie lub w szafie zamykanej na klucz lub w innych ustalonych w planie, odizolowanych od ingerencji zewnętrznej miejscach.
20. W przypadku kopii zapasowych danych osobowych mających szczególną wartość dla kancelarii wykonuje się wielokrotne kopie, na oddzielnych nośnikach, które przechowywane są w różnych lokalizacjach, w celu zmniejszenia możliwości utraty istotnych informacji. Ponadto wszystkie kopie zapasowe, o ile to możliwe, przechowywane są w innych lokalizacjach niż dane, z których zostały wykonane.
21. Kopie zapasowe mające szczególną wartość dla kancelarii należy przechowywać w miejscach, które minimalizują możliwość ich utraty w przypadku wystąpienia zdarzeń losowych mogących je zniszczyć (np. powódź, pożar, itp.).
22. Kopie zapasowe przechowywane są przez okres minimum 7 dni. Kopie zapasowe nie mogą być przechowywane po ustaniu celu przetwarzania danych osobowych na nich zawartych.
23. Dostęp do kopii zapasowych jest ograniczony jedynie dla Administratora lub osoby przez niego wyznaczonej.

24. Udostępnienie informacji odtworzonych z kopii zapasowej odbywa się pod nadzorem Administratora.

§ 15

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Sieć lokalna kancelarii jest odpowiednio zarządzana i nadzorowana, aby ochronić ją przed zagrożeniami oraz utrzymywać bezpieczeństwo systemów teleinformatycznych i urządzeń sieciowych. Przesyłanie danych pomiędzy stacjami roboczymi kancelarii nie powinno odbywać się przez sieć publiczną, chyba, że odbywa się bezpiecznymi kanałami szyfrowania w technologii VPN.
2. Na stacjach roboczych, przenośnych komputerach osobistych, serwerach oraz bramkach pocztowych instaluje się system antywirusowy wykrywający aplikacje lub skrypty, których celem jest złośliwe, szkodliwe bądź przestępcze działanie mogące naruszyć poufność, integralność lub dostępność informacji.
3. Żadne oprogramowanie oraz nośniki danych nie mogą być użyte bez wcześniejszego sprawdzenia przy pomocy odpowiedniego oprogramowania antywirusowego.
4. Oprogramowanie używane w kancelarii powinno być na bieżąco aktualizowane.

IV. POSTANOWIENIA KOŃCOWE

§ 16

1. Aktualizacji niniejszej polityki dokonuje Administrator.
2. Poszczególne postanowienia niniejszej polityki mogą być na bieżąco zmieniane i dostosowywane przez Administratora do potrzeb kancelarii.
3. W przypadku istotnej zmiany zakresu przetwarzania danych osobowych w kancelarii lub sposobu ich przetwarzania, Administrator podejmuje działania zmierzające do analizy wpływu tych zmian na potrzebę zmiany niniejszej polityki.
4. Po zmianie polityki, Administrator zapoznaje pracowników ze zmianami.

§ 17

Polityka obowiązuje od 26 maja 2025 roku

Notariusz

Grzegorz Mrowiński