KANCELARIA ADWOKACKA ADWOKAT ANDRZEJ ŚWIĄDER

ul. Oszczepowa 83, 94 – 123 Łódź

tel./fax (42) 689 01 41

tel. kom. 608385052

e-mail: kontakt@kancelaria-swiader.pl

www.kancelaria-swiader.pl

POLITYKA BEZPIECZEŃSTWA INFORMACJI

w

KANCELARII ADWOKACKIEJ ADWOKATA ANDRZEJA ŚWIĄDRA

Maj 2018

Niniejsza Polityka bezpieczeństwa, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w kancelarii, w tym z Rozporządzeniem 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)

I. Informacje ogólne.

1. Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania Kancelarii Adwokackiej Adwokata Andrzeja Świądra jako Administratora Danych Osobowych z przepisami prawa regulującymi kwestię administrowania i przetwarzania danych osobowych. Niniejsza Polityka Bezpieczeństwa opisuje w szczególności zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.
2. Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:
    a. Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922);
    b. Rozporządzeniu 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];
    c. Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 nr 100 poz. 1024),
4. Obszar, w którym przetwarzane są Dane osobowe na terenie Kancelarii Adwokackiej Adwokata Andrzeja Świąder obejmuje:
    a. pomieszczenie biurowe kancelarii zlokalizowane w Łodzi (90-553) ul. Mikołaja Kopernika 72 lok. 171.,

b. pomieszczenie biurowe kancelarii zlokalizowane w Łodzi (94-123) ul. Oszczepowa 83,

c. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym w punkcie 4 lit. a -b.

5. Ochrona danych osobowych realizowana jest poprzez stosowanie zabezpieczeń w postaci środków organizacyjnych, środków ochrony fizycznej oraz środków technicznych systemu informatycznego w ramach procedur zawartych w instrukcji zarządzania systemem informatycznym.

5. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Kancelarii Adwokackiej Adwokata Andrzeja Świądra rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.

6. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów:

a. Poufność danych – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,

b. Integralność danych – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

c. Dostępność danych – zapewnienie osiągalności danych i możliwości ich wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,

d. Rozliczalność danych – zapewnienie, że działania podmiotu mogą być przy pisane w sposób jednoznaczny tylko temu podmiotowi,

e. Autentyczność danych – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,

f. Integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;

g. Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

7. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
8. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.
9. Zgodnie z art. 6 ustawy z 26 maja 1982 r. Prawo o Adwokaturze (tekst jednolity: Dz. U. z 2017 r. poz. 2368) Dane osobowe przetwarzane w Kancelarii Adwokackiej Adwokata Andrzeja Świąder, a uzyskane w związku z udzielaniem pomocy prawnej przez adwokata, objęte są tajemnicą adwokacką. Adwokata nie można zwolnić od obowiązku zachowania tajemnicy zawodowej co do faktów, o których dowiedział się udzielając pomocy prawnej lub prowadząc sprawę.
10. W zakresie przetwarzania danych pozyskanych w związku z wykonywaniem czynności objętych tajemnicą adwokacką Administrator stosuje się do wskazanych powyżej przepisów dotyczących zachowania tajemnicy zawodowej.

II. Definicje.

Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

1) Polityka Bezpieczeństwa – rozumie się przez to Politykę Bezpieczeństwa Informacji w Kancelarii Adwokackiej Adwokata Andrzeja Świądra;
2) Administrator Danych Osobowych – Administratorem Danych Osobowych w rozumieniu niniejszej Polityki Bezpieczeństwa jest Adwokat Andrzej Świąder prowadzący działalność gospodarczą pod firmą „Kancelaria Adwokacka" Andrzej Świąder;
3) Kancelaria – siedziba Kancelarii Adwokackiej Adwokata Andrzeja Świądra
4) Ustawa – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922);
5) Rozporządzenie – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) z późniejszymi zmianami;
6) 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 [rozporządzenie ogólne o ochronie danych];
7) Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
8) Zbiór danych osobowych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych

kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

9) Baza danych osobowych – zbiór uporządkowanych powiązanych ze sobą tematycznie zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;
10) Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą.
11) Przetwarzanie danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
12) System informatyczny - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
13) Bezpieczeństwo systemu informatycznego – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed nieuprawnionym przetwarzaniem danych;
14) Użytkownik - rozumie się przez to osobę wyznaczoną i upoważnioną przez Administratora danych do przetwarzania danych osobowych, przeszkoloną w zakresie ochrony tych danych;
15) Stacja robocza – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie;

16) Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie;
17) Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie;
18) Państwo trzecie – rozumie się przez to każde państwo nienależące do Europejskiego Obszaru Gospodarczego (zwanego dalej: EOG).

III. Dokumenty powiązane.

Dokumentem powiązanym z Polityką bezpieczeństwa przetwarzania danych osobowych w Kancelarii Adwokackiej Adwokata Andrzeja Świąder jest, zgodnie z wymogami § 3 ust. 1 Rozporządzenia, Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Kancelarii Adwokackiej Adwokata Andrzeja Świąder.

IV. Dane osobowe przetwarzane u administratora danych.

1. Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych.
2. Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.

3. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
4. Administrator danych prowadzi rejestr czynności przetwarzania. Wzór rejestru czynności przetwarzania stanowi Załącznik nr 1 do niniejszej polityki.

V. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem.

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Polityką Bezpieczeństwa, Instrukcją Zarządzania Systemem Informatycznym, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych w Kancelarii Adwokackiej Adwokata Andrzeja Świąder.
2. Wszystkie dane osobowe w Kancelarii są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
    a) W każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych.
    b) Dane są przetwarzane są rzetelnie i w sposób przejrzysty.
    c) Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
    d) Dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych.
    e) Dane osobowe są prawidłowe i w razie potrzeby uaktualniane.

f) Czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane.

g) Wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO.

h) Dane są zabezpieczone przed naruszeniami zasad ich ochrony.

3. Do najważniejszych obowiązków Administratora Danych Osobowych należy:

a) Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych oraz innych przepisów regulujących zasady bezpieczeństwa i ochrony danych osobowych;

b) Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa;

c) Wydawanie i anulowanie upoważnień do przetwarzania danych osobowych;

d) Przeprowadzanie szkoleń użytkowników przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe;

e) Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;

f) Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;

g) Nadzór nad bezpieczeństwem danych osobowych;

h) Kontrola działań pracowników pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;

i) Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;

j) Bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych;

k) Optymalizację wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego;

l) Instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego;

m) Konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem;

n) Współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych;

o) Zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego oraz sieciowego;

p) Przeciwdziałanie próbom naruszenia bezpieczeństwa informacji;

q) Zmiana lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń;

r) Zarządzanie licencjami oraz procedurami ich dotyczącymi;

s) Prowadzenie profilaktyki antywirusowej.

4. Do najważniejszych obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

a) Znajomość, zrozumienie i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony danych osobowych oraz uniemożliwienie osobom nieuprawnionym dostępu do swojej stacji roboczej;

b) Przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami;

c) Postępowania zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych;

d) Zachowania w tajemnicy danych osobowych, do których uzyskały dostęp oraz informacji o sposobach ich zabezpieczenia;

e) Ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;

f) Informowania Administratora Danych Osobowych o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe;

g) Zapoznanie się z Polityką Bezpieczeństwa przetwarzania danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

VI. Zarządzanie ochroną danych osobowych.

1. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z upoważnieniem oraz rolą sprawowaną w procesie przetwarzania danych.
2. Dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej.
3. Każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia.

4. Należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych.
5. Należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.
6. Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.
7. Dane osobowe należy przetwarzać wyłącznie za pomocą autoryzowanych urządzeń służbowych.
8. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane na mocy art. 32 RODO albo art. 37 Ustawy. Upoważnienia wydawane są indywidualnie przez Administratora Danych Osobowych

VII. Szkolenia użytkowników.

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada Administrator Danych Osobowych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi, RODO oraz Polityką Bezpieczeństwa Informacji i Instrukcją zarządzania systemem informatycznym służącym do

przetwarzania danych osobowych obowiązującymi u Administratora Danych. Po zaznajomieniu się z powyższymi regulacjami, użytkownik, przed dopuszczeniem do przetwarzania danych, powinien zobowiązać się do ich przestrzegania przez podpisanie oświadczenia użytkownika, stanowiącego załącznik nr 3 do Polityki Bezpieczeństwa.

VIII. Powierzenie przetwarzania danych osobowych.

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO i tylko jeżeli są to dane, które może ujawnić bez naruszenia adwokackiej tajemnicy zawodowej.
2. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.
3. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

IX. Przekazywanie danych do państwa trzeciego.

Administrator Danych Osobowych nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą.

X. Udostępnianie danych osobowych.

1. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.
2. Udostępnianie danych osobowych może nastąpić wyłącznie za zgodą Administratora Danych Osobowych.
3. Informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru listem poleconym za pokwitowaniem odbioru lub innym bezpiecznym sposobem, określonym wymogiem prawnym lub umową.
4. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

XI. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych, Środki te obejmują:
    a. Ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do

przetwarzania danych jedynie w towarzystwie osoby upoważnionej. Polityka bezpieczeństwa informacji.

b. Zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w pkt I. 4 powyżej na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich.
c. Wykorzystanie zamykanych szafek i sejfów do zabezpieczenia dokumentów.
d. Wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe.
e. Ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall.
f. Ochronę sprzętu komputerowego wykorzystywanego u administratora przed złośliwym oprogramowaniem.
g. Zabezpieczenie dostępu do urządzeń Kancelarii przy pomocy haseł dostępu.
h. Wykorzystanie szyfrowania danych przy ich transmisji.

XII. Naruszenie zasad ochrony danych osobowych.

1. Każdy użytkownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest o tym poinformować Administratora Danych.
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
    a. Niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;

b. Niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;

c. Nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.

3. Do typowych incydentów bezpieczeństwa danych osobowych należą:

   a. Zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);

   b. Zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych);

   c. Umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.

5. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Wzór zgłoszenia określa załącznik nr 3 do niniejszej polityki.

6. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

XIII. Postanowienia końcowe.

1. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, Przepisów o ochronie danych osobowych oraz Kodeksu karnego w odniesieniu do danych osobowych objętych tajemnicą zawodową.
2. Integralną część niniejszej Polityki bezpieczeństwa stanowią następujące Załączniki:
    a. Rejestr czynności przetwarzania danych osobowych;
    b. Wzór upoważnienia do przetwarzania danych osobowych;
    c. Wzór Oświadczenia i zobowiązania osoby przetwarzającej dane osobowe;
    d. Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego.

Niniejsza Polityka bezpieczeństwa, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w kancelarii, w tym z Rozporządzeniem 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)

Załącznik – Rejestr czynności przetwarzania

Rejestr czynności przetwarzania – przykład		
Dane administratora (imię, nazwisko/ nazwa, dane kontaktowe):	**Kancelaria Adwokacka Adwokat Andrzej Świąder ul. Oszczepowa 83 94-123 Łódź +48608385052 kontakt@kancelaria-swiader.pl**	
Dane inspektora ochrony danych lub osoby odpowiedzialnej za ochronę danych osobowych u administratora, jeżeli została wyznaczona (imię, nazwisko, dane kontaktowe):		
Osoba odpowiedzialna za aktualizację rejestru:	**Adwokat Andrzej Świąder**	
Nazwa procesu (czynność przetwarzania):		**Numer wpisu:**
Cel przetwarzania danych		
Charakter przetwarzania danych		
Podstawa przetwarzania		
Kategorie osób, których dane dotyczą		
Zakres przetwarzanych danych według kategorii danych	Dane identyfikacyjne	
	Dane identyfikacyjne sensytywne	
	Dane kontaktowe	

Kontekst przetwarzanych danych		
Kategorie odbiorców / Odbiorcy danych		
Transfery danych		
Retencja		
Opis środków technicznych i organizacyjnych	1. Zabezpieczenia organizacyjne: a) Upoważnienia do przetwarzania danych b) Oświadczenie o zachowaniu poufności c) Szkolenie z zakresu ochrony danych d) Podpisanie umowy powierzenia e) Dokonywanie przeglądów stosowanych procedur f) Wdrożenie odpowiednich polityk retencyjnych g) Wdrożenie odpowiednich polityk informacyjnych 2. Zabezpieczenia informatyczne i fizyczne: a) anonimizacja, usuwanie danych b) backupy danych c) blokada USB, napędów optycznych d) indywidualne konta w systemie operacyjnym / indywidualne konta w programach przetwarzających dane e) legalność oprogramowania	

	f) logowanie operacji na danych osobowych g) niszczenie nośników / niszczenie wydruków h) ochrona przed zanikiem zasilania i) lokalizacja stanowisk komputerowych j) polityka kluczy - dostęp do pomieszczeń k) postępowanie z komputerami przenośnymi l) poziomy uprawnień w programach (użytkowników) m) poziomy uprawnień administratorów (serwery) n) procedura korzystania z poczty elektronicznej / procedura korzystania z Internetu / procedury pracy przy stanowisku komputerowym o) programy antywirusowe, firewalle p) szyfrowanie transmisji / szyfrowanie dysków / szyfrowanie plików zapisywanych na nośnikach q) wydzielone miejsca przechowywania dokumentów i nośników danych
Informacje dodatkowe np. proces uprzednich konsultacji, zastosowanie kodeksu dobrych praktyk, certyfikacja	
Data wpisu / modyfikacja wpisu	
Data wykreślenia z rejestru	

Załącznik – Wzór upoważnienia do przetwarzania danych osobowych

....., dn. ..... r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

nr .....

Działając w imieniu ..... niniejszym upoważniam: Panią/Pana .....Stanowisko ..... do przetwarzania danych osobowych w Kancelarii Adwokackiej Adwokata Andrzeja Świąder w następującym zakresie*:

A. Okres upoważnienia:

na okres zatrudnienia / współpracy z ..... do dnia ..... włącznie.

B. Zakres upoważnienia:
   a. dane przetwarzane na nośnikach papierowych,
   b. system informatyczny,
   c. dane osobowe objęte zbiorem:
      i. .....
      ii. .....
      iii. .....

* bez ograniczeń, podgląd danych, wprowadzanie danych, opracowywanie danych, zmienianie danych, usuwanie danych, na komputerach przenośnych) [należy pozostawić właściwe]

.....

Adwokat Andrzej Świąder

Załącznik – Wzór oświadczenia i zobowiązania osoby przetwarzającej dane osobowe

....., dn. ..... r.

.....

imię i nazwisko osoby upoważnionej

.....

stanowisko

Kancelaria Adwokacka Adwokata Andrzeja Świąder

ul. Mikołaja Kopernika 72 lok. 171

90 – 553 Łódź

miejsce pracy

OŚWIADCZENIE

Oświadczam, że – w związku z wykonywaniem przeze mnie prac na rzecz Kancelarii Adwokackiej Adwokata Andrzeja Świądra i upoważnieniem mnie do Przetwarzania danych osobowych – zostałem/łam zapoznany/a ze stosownymi przepisami i standardami ochrony danych osobowych, zobowiązuję się do przestrzegania:

a. Przepisów o ochronie adwokackiej tajemnicy zawodowej w tym m.in.:
    i. Ustawy z dnia 26 maja 1982 roku Prawo o adwokaturze (tekst jednolity: Dz. U. z 2017 r. poz. 2368),

ii. Zbioru Zasad Etyki Adwokackiej i Godności Zawodu (Kodeks Etyki Adwokackiej)

b. Przepisów o ochronie danych osobowych, w tym 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.

c. Przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. Nr 133, poz. 883)

d. Polityki Bezpieczeństwa informacji w Kancelarii Adwokackiej Adwokata Andrzeja Świąder

e. Instrukcji zarządzania systemem Informatycznym w Kancelarii Adwokackiej Adwokata Andrzeja Świąder.

f. W związku z powyższym zobowiązuję się do:

a) zapewnienia ochrony danych osobowych przetwarzanych w zbiorach administratora, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,

b) zachowania w tajemnicy, także po zaprzestaniu wykonywania prac, wszelkich informacji dotyczących funkcjonowania systemów służących do przetwarzania danych osobowych w zbiorach .....

c) natychmiastowego zgłaszania do Administratora Danych zaobserwowania próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa zbioru/zbiorów lub systemów informatycznych.

.....

[podpis pracownika/współpracownika

Załącznik - Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego.

Data, miejscowość

Nadawca:

.....

.....

.....

Adresat:

.....

.....

.....

Zgłoszenie naruszenia ochrony danych osobowych

w trybie art. 33 rozporządzenia 2016/679

Na podstawie art. 33 ogólnego rozporządzenia o ochronie danych, działając w imieniu administratora .....informuję, że stwierdzono, iż w dniu .....* doszło w strukturze administratora do naruszenia bezpieczeństwa danych osobowych, opisanego poniżej, zgodnie z wymogami wyżej wskazanego przepisu art. 33.

*Przyczyny uzasadniające dokonanie zgłoszenia po upływie 72 godzin od ich wykrycia: .....

Osobą odpowiedzialną za bezpieczeństwo danych osobowych w strukturze administratora jest:..... / adres ..... / adres e-mail/ nr telefonu ..... .

Zgłaszane naruszenie dotyczy procesu przetwarzania, określonego w organizacji jako .....

Niezwłocznie po zaistnieniu podejrzenia wystąpienia naruszenia administrator podjął czynności wyjaśniająco-naprawcze, w toku których ustalił następujące okoliczności zdarzenia:

1. Okoliczności naruszenia:.....
2. Kategorie osób, których dane dotyczą, dotkniętych naruszeniem:.....
3. Liczba osób, których dane dotyczą, dotkniętych naruszeniem:.....
4. Kategorie danych osobowych dotkniętych naruszeniem:.....
5. Liczba wpisów danych osobowych dotkniętych naruszeniem:.....

Podsumowanie ustaleń administratora zamieszczono w tabeli poniżej:

LP.	DATA NARUSZENIA	NAZWA PROCESU DANYCH OSOBOWYCH	SYSTEM / NARZĘDZIA	ZAKRES NARUSZENIA DANYCH
1				
2				

Administrator zidentyfikował następujące, możliwe konsekwencje naruszenia ochrony danych osobowych:

1. Dla organizacji: .....
2. Dla osób, których dane dotyczą: .....

Administrator podjął następujące działania *ad hoc*, niezwłocznie po zaistnieniu podejrzenia wystąpienia naruszenia: ..... Natomiast niezwłocznie po stwierdzeniu, że doszło do naruszenia, podjęto następujące działania naprawcze: .....

Administrator sformułował także zalecenia naprawcze i plan działania w celu zminimalizowania konsekwencji naruszenia oraz w celu zaradzenia powstania analogicznego naruszenia w przyszłości
.....
.....
.....
.....

W celu zminimalizowania negatywnych skutków naruszenia dla osób, których dane dotyczą administrator powziął /rekomendował następujące działania:
.....
.....
.....

Podpis: .....

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz zarządzania polityką bezpieczeństwa w Kancelarii Adwokackiej Adwokata Andrzeja Świądra

Stosownie do postanowień § 4 i 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024 ze zm.), ustala się treść Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych polityki bezpieczeństwa, która znajdzie zastosowanie do danych osobowych przetwarzanych w systemie informatycznym oraz na innych nośnikach informacji w Kancelarii Adwokackiej Adwokata Andrzeja Świądra zwanej dalej „KANCELARIĄ ADWOKACKĄ".

Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych Kancelarii Adwokackiej przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 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).

Niniejsza Polityka bezpieczeństwa, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w kancelarii, w tym z Rozporządzeniem 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)

Definicje:

1. Administrator Danych Kancelaria Adwokacka Adwokat Andrzej Świąder.
2. Dane osobowe – wszelkie informacje, w tym o stanie zdrowia, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
3. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu Przetwarzania danych.
4. Użytkownik – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych w Kancelarii Adwokackiej Adwokata Andrzeja Świąder.
5. Sieć lokalna – połączenie Systemów informatycznych Administratora Danych wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
6. Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
7. Przetwarzanie danych – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w Systemach informatycznych.
8. Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym Przetwarzaniem.
9. Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do Przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie.
10. Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym (Użytkownikowi).

I. Procedury nadawania uprawnień do Przetwarzania danych i rejestrowania tych uprawnień w Systemie informatycznym

1. Za bezpieczeństwo Danych osobowych w Systemie informatycznym Kancelarii Adwokackiej Adwokata Andrzeja Świąder (Windows 10 Pro, Windows 7) i za właściwy nadzór odpowiedzialny jest Administrator Danych.
2. Do obsługi Systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do Przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez Administratora Danych.
3. Po upoważnieniu osoby do dostępu do przetwarzania danych osobowych w systemie informatycznym zostaje jej nadany Identyfikator użytkownika. Z chwilą nadania Identyfikatora osoba może uzyskać dostęp do systemów informatycznych w zakresie odpowiednim do danego upoważnienia.
4. Dla każdego Użytkownika Systemu informatycznego ustalony jest odrębny Identyfikator i Hasło.
5. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu Użytkownika z Systemu informatycznego nie może być przydzielony innej osobie.
6. Identyfikator osoby, która utraciła uprawnienia do dostępu do Danych osobowych, zostaje niezwłocznie wyrejestrowany z Systemu informatycznego, w którym są przetwarzane, zaś Hasło dostępu zostaje unieważnione oraz zostają podjęte inne działania niezbędne w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

II. Metody i środki Uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. W Systemie informatycznym stosuje się Uwierzytelnianie na poziomie dostępu do systemu operacyjnego. Do Uwierzytelnienia Użytkownika na poziomie dostępu do systemu operacyjnego stosuje się Hasło oraz Identyfikator użytkownika.
2. Hasła użytkowników umożliwiające dostęp do Systemu informatycznego utrzymuje się w tajemnicy również po upływie ich ważności.
3. Minimalna długość Hasła przydzielonego Użytkownikowi wynosi osiem znaków alfanumerycznych i znaków specjalnych.
4. Zabrania się używania identyfikatora lub Hasła drugiej osoby.
5. Dla każdej osoby, której Dane osobowe są przetwarzane w Systemie informatycznym, system zapewnia odnotowanie:

a. daty pierwszego wprowadzenia danych do systemu,
b. identyfikatora Użytkownika wprowadzającego Dane osobowe do systemu,
c. informacji o odbiorcach, którym Dane osobowe zostały udostępnione.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez Użytkowników systemu

1. Pracownik po przyjściu do pracy uruchamia stację roboczą.
2. Przed uruchomieniem komputera należy sprawdzić, czy nie zostały do niego podłączone żadne niezidentyfikowane urządzenia.
3. Po uruchomieniu pracownik loguje się przy pomocy identyfikatora Użytkownika oraz hasła do systemu informatycznego.
4. W trakcie pracy przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane Dane osobowe.
5. Przy opuszczaniu stanowiska na dłuższy czas należy ustawić ręcznie blokadę klawiatury i wygaszacz ekranu (wygaszacz nie rzadszy niż aktywujący się po 15 min braku aktywności).

IV. Tworzenie kopii zapasowych Zbiorów danych

1. Dla zabezpieczenia integralności danych dokonuje się archiwizacji danych w systemach Kancelarii.
2. Do archiwizacji służy przenośny dysk twardy o pojemności 1 Tb.
3. Wszystkie dane archiwizowane winny być identyfikowane, tj. zawierać takie informacje jak datę dokonania zapisu oraz identyfikator zapisanych w kopii danych.

V. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających Dane osobowe oraz kopii zapasowych

1. Nośniki z kopiami archiwalnymi powinny być zabezpieczone przed dostępem do nich osób nieupoważnionych, przed zniszczeniem czy kradzieżą.

2. Nośników z danymi zarchiwizowanymi nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są Zbiory danych osobowych używane na bieżąco.
3. Nośniki informacji, kopie zapasowe, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
4. Kopie, które są już nieprzydatne, należy zniszczyć fizycznie lub stosując wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane kasowane.
5. Zabrania się wynoszenia jakichkolwiek nagranych nośników zawierających dane osobowe z miejsca pracy.

VI. Sposób zabezpieczenia Systemu informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awariami zasilania

1. System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej. Zabezpieczenie obejmuje:

	Obszar chroniony	Rodzaj ochrony	Typ
1. 2. 3.	Stacje robocze	System antywirusowy	Bitdefender Total Security 2018
		Firewall	Bitdefender Total Security 2018
		Szyfrowanie nośników danych	VeraCrypt
4. 5.	Sieć wewnętrzna	System antywirusowy	X
		Firewall	Firewall w Routerze

			TP-LINK
6. . 7.	Poczta e-mail	Szyfrowanie danych	SSL/TLS
		System antywirusowy i antyspamowy	Bitdefender Total Security 2018

2. Użytkowany system jest automatycznie skanowany z częstotliwością jeden raz na miesiąc.
3. Aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy.
4. W przypadku wykrycia wirusa należy: a) uruchomić program antywirusowy i skontrolować użytkowany system, b) usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego. Jeżeli operacja usunięcia wirusa się nie powiedzie, należy: a) zakończyć pracę w systemie komputerowym, b) odłączyć zainfekowany komputer od sieci, c) powiadomić o zaistniałej sytuacji Administratora Danych lub ABI.
5. Urządzenia i nośniki zawierające Dane osobowe przekazywane poza obszar, w którym są one przetwarzane, zabezpiecza się w sposób zapewniający poufność i integralność danych.

VII. Poczta elektroniczna

1. Pracownicy mogą korzystać z poczty elektronicznej w celach służbowych oraz w celach prywatnych w zakresie ograniczonym swoimi obowiązkami.
2. Administrator może poznawać treść wiadomości elektronicznych wykorzystywanych przez pracowników znajdujących się we wszystkich systemach Administratora. 3. Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem (tzw. phishing e-mail). W szczególności zabronione jest otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.

VIII. Sposoby realizacji w systemie wymogów dotyczących Przetwarzania danych (sposób realizacji wymogu zapisania w Systemie informatycznym informacji o odbiorcach danych)

1. Informacje o odbiorcach danych zapisywane są w Systemie informatycznym, z którego nastąpiło udostępnienie.
2. Informacja o odbiorcy danych zapisana jest w Systemie informatycznym przy uwzględnianiu daty i zakresu udostępnienia, a także dokładnego określenia odbiorcy danych.
3. Możliwe jest sporządzenie i wydrukowanie raportu zawierającego, w powszechnie zrozumiałej formie, powyższe informacje.

IX. Procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do Przetwarzania danych

1. Przeglądy kontrolne, serwis sprzętu i oprogramowania powinny być dokonywane przez firmy serwisowe, z którymi zostały zawarte umowy zawierające postanowienia zobowiązujące je do przestrzegania zasad poufności informacji uzyskanych w ramach wykonywanych zadań.
2. Przy dokonywaniu serwisu należy przestrzegać następujących zasad:
   a) czynności serwisowe powinny być wykonywane w obecności osoby upoważnionej do Przetwarzania danych,
   b) przed rozpoczęciem tych czynności dane i programy znajdujące się w systemie powinny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą,
   c) prace serwisowe należy ewidencjonować w książce zawierającej rodzaj wykonywanych czynności serwisowych, daty rozpoczęcia i zakończenia usługi, odnotowanie osób dokonujących czynności serwisowych, tj. imienia i nazwiska, a także osób uczestniczących w pracach serwisowych,
   d) w przypadku prac serwisowych dokonywanych przez podmiot zewnętrzny, wymagających dostępu do Danych osobowych, z podmiotem takim powinny zostać zawarte stosowne umowy powierzenia danych osobowych.