POLITYKA BEZPIECZEŃSTWA INFORMACJI

w

KANCELARII
FORYSTEK & PARTNERZY
ADWOKACI I RADCOWIE PRAWNI

WPROWADZONO:

DNIA 24 MAJA 2018 ROKU

KRAKÓW

I. POSTANOWIENIA OGÓLNE

1. Polityka Bezpieczeństwa Informacji została sporządzona w celu zapewnienia zgodności przetwarzania danych osobowych w **Kancelarii Forystek & Partnerzy Adwokaci i Radcowie Prawni** z obowiązkami wynikającymi z przepisów prawa regulujących zasady przetwarzania, zabezpieczania i ochrony danych osobowych.
2. Niniejszy dokument został sporządzony zgodnie z wymaganiami wprowadzonymi Rozporządzeniem Parlamentu Europejskiego i Radu (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony danych osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „**RODO**"), ustawą z dnia 10 maja 2018 roku o ochronie danych osobowych oraz założeniami projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679, wraz z przepisami wykonawczymi.
3. Polityka Bezpieczeństwa Informacji reguluje sposób przetwarzania danych osobowych niezależnie od formy ich przetwarzania oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.
4. Polityka Bezpieczeństwa Informacji dotyczy wszelkich danych osobowych przetwarzanych w ramach działalności Kancelarii i obowiązuje we wszystkich komórkach organizacyjnych Kancelarii.
5. Polityka Bezpieczeństwa Informacji przechowywana jest w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
6. Polityka Bezpieczeństwa Informacji udostępniana jest do wglądu na wniosek osób posiadających stosowne upoważnienie do przetwarzania danych osobowych. Polityka Bezpieczeństwa Informacji udostępniana jest także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych celem umożliwienia zapoznania się z jej treścią. Upoważnienie do przetwarzania danych osobowych nadawane jest po uprzednim zapoznaniu osoby, której nadawane jest upoważnienie z treścią Polityki Bezpieczeństwa Informacji.
7. Celem Administratora jest wdrożenie rozwiązań organizacyjnych i dostępnych zabezpieczeń technicznych umożliwiających spełnienie wymagań w zakresie przetwarzania danych osobowych. Administrator w szczególności dąży do dostosowania przyjętych rozwiązań w zakresie następujących nadrzędnych zasad, które Administrator uznaje za kluczowe dla prawidłowej ochrony danych osobowych:
    a) **zgodność z prawem, rzetelność i przejrzystość** – rozumianą jako przetwarzanie danych osobowych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
    b) **ograniczenie celu** – rozumianą jako zbieranie danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane ich dalej w sposób niezgodny z tymi celami;

c) **minimalizacja danych** – rozumianą jako przetwarzanie danych osobowych w sposób adekwatny, stosowny oraz ograniczony do tego, co jest niezbędne do celów, w których dane są przetwarzane;
d) **prawidłowość danych** – rozumianą jako przetwarzanie prawidłowych i w razie potrzeby uaktualnionych danych osobowych;
e) **ograniczenie przechowywania** – rozumianą jako przechowywanie danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane
f) **integralność i poufność** – rozumianą jako przetwarzanie danych w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych

8. Dla skutecznej realizacji Polityki Bezpieczeństwa Informacji Administrator zapewnia:
   a) stosowanie odpowiednich do zagrożeń i kategorii danych osobowych objętych ochroną środki techniczne i rozwiązania organizacyjne.
   b) kontrolę i nadzór nad przetwarzaniem danych osobowych w ramach Kancelarii;
   c) monitorowanie zastosowanych środków ochrony danych;
9. Monitorowanie przez Administratora zastosowanych środków ochrony obejmuje m.in. działania osób upoważnionych do przetwarzania danych osobowych, działania podmiotów przetwarzających dane osobowe w imieniu Administratora, kontrolę naruszeń zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi, w tym w szczególności atakami na system informatyczny Administratora.
10. Administrator zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych w Kancelarii są zgodne z Polityką Bezpieczeństwa Informacji oraz odpowiednimi przepisami prawa.

II. DEFINICJE

1. Na potrzeby Polityki Bezpieczeństwa Informacji, zwrotom wymienionym poniżej nadaje się następujące znaczenie:

   a) **Administrator** – Forystek i Partnerzy Adwokaci i Radcowie Prawni spółka partnerska z siedzibą w Krakowie, ul. Grzegórzecka 21 (31-532 Kraków), wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Krakowa-Śródmieścia w

Krakowie, XI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000179150, NIP: 6772219730;

b) **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

c) **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie teleinformatycznym (użytkownikowi) w razie przetwarzania danych osobowych w takim systemie;

d) **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby przetwarzającej dane osobowe;

e) **Użytkownik** – osoba upoważniona przez Administratora do przetwarzania danych osobowych;

f) **Przetwarzanie danych** – są to jakiekolwiek operacje wykonywane na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak w szczególności:

- Zbieranie;
- Utrwalanie;
- Organizowanie;
- Porządkowanie;
- Przechowywanie;
- Adaptowanie lub modyfikowanie;
- Pobieranie;
- Przeglądanie;
- Wykorzystywanie;
- Ujawnianie poprzez przesłanie;
- Rozpowszechnianie lub innego rodzaju udostępnianie;
- Dopasowywanie lub łączenie;
- Ograniczanie;
- Usuwanie;
- Niszczenie.

g) **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych;

h) **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

III. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Administratorem danych osobowych jest Forystek & Partnerzy Adwokaci i Radcowie Prawni Spółka Partnerska z siedzibą w Krakowie, ul. Grzegórzecka 21 (31-532 Kraków), wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie, XI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000179150, NIP: 6772219730.
2. Wszystkie dane osobowe w Kancelarii są przetwarzane z poszanowaniem zasad przetwarzania danych osobowych przewidzianych przez przepisy prawa, w szczególności:
   a) **przetwarzanie danych następuje wyłącznie w sytuacji, gdy spełniona została chociaż jedna z przewidzianych przepisami prawa podstaw przetwarzania danych osobowych**, a mianowicie:
      - osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
      - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy;
      - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze;
      - przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
      - przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
      - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa

i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

b) przetwarzanie danych osobowych następuje w sposób rzetelny oraz przejrzysty;
c) przetwarzanie danych osobowych następuje w konkretnych, wyraźnych oraz prawnie uzasadnionych celach. Przetwarzanie danych osobowych w sposób niezgodny z tymi celami jest zabronione;
d) przetwarzanie danych osobowych następuje jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych osobowych;
e) przetwarzane dane osobowe są prawidłowe. W razie potrzeby przetwarzane dane osobowe podlegają uaktualnieniu;
f) przetwarzanie danych osobowych jest ograniczone do okresu przydatności do celów, dla jakich zostały zebrane. Po upływie tego okresu dane są anonimizowane bądź usuwane.
g) przetwarzanie danych osobowych jest dopuszczalne po spełnieniu obowiązku informacyjnego określonego w art. 13 i 14 RODO, o ile spełnienie takiego obowiązku informacyjnego jest wymagane.

3. Dane osobowe przetwarzane są przez Administratora w formie papierowej oraz elektronicznej.
4. Administrator jest odpowiedzialny za prawidłowe przetwarzanie danych osobowych. W tym celu Administrator podejmuje wszelkie działania umożliwiające spełnienie oraz wykazanie spełnienia wymagań wynikających z zasad przetwarzania danych osobowych.
5. Zgodnie z art. 6 ustawy z 26 maja 1982 r. Prawo o Adwokaturze, dane osobowe przetwarzane w Kancelarii Forystek & Partnerzy Adwokaci i Radcowie Prawni 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.
6. Zgodnie z art. 3 ust. 3 ustawy z dnia 6 lipca 1982 r. o Radcach Prawnych, dane osobowe przetwarzane w Kancelarii Forystek & Partnerzy Adwokaci i Radcowie Prawni a uzyskane w związku z udzielaniem pomocy prawnej przez radcę prawnego, objęte są tajemnicą radcowską. Radcy prawnego nie można zwolnić od obowiązku zachowania tajemnicy zawodowej co do faktów, o których dowiedział się udzielając pomocy prawnej lub prowadząc sprawę.
7. W zakresie przetwarzania danych pozyskanych w związku z wykonywaniem czynności objętych tajemnicą adwokacką lub tajemnicą radcowską, Administrator stosuje się do wskazanych powyżej przepisów dotyczących zachowania tajemnicy zawodowej.

8. 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.
9. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania (*privacy by design*).
10. Administrator prowadzi Rejestr Czynności Przetwarzania zgodnie z **Załącznikiem nr 4** do Polityki Bezpieczeństwa Informacji.

IV. 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 Polityką Bezpieczeństwa Informacji, Instrukcją Zarządzania Systemem Informatycznym stanowiącą **Załącznik nr 1**, Polityką czystego biurka opisaną w **Załączniku nr 3**, a także innymi dokumentami wewnętrznymi i procedurami związanymi z przetwarzaniem danych osobowych w Kancelarii Forystek & Partnerzy Adwokaci i Radcowie Prawni.
2. Administrator nie przekazuje osobom, których dane dotyczą, informacji w sytuacji, w której dane te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej (art. 14 ust. 5 pkt d RODO)
3. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony danych osobowych uważa się w szczególności:
    a) naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach;
    b) udostępnianie lub umożliwienie udostępnienia danych osobom lub podmiotom do tego nieupoważnionym;
    c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
    d) niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
    e) przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;
    f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych;
    g) naruszenie praw osób, których dane są przetwarzane.

4. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora.
5. Do obowiązków Administratora w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora na podstawie innych umów cywilnoprawnych) należy dopilnowanie, by:
    a) pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków,
    b) każdy z przetwarzających dane osobowe był pisemnie upoważniony do przetwarzania zgodnie z Upoważnieniem do przetwarzania danych osobowych stanowiącym **Załącznik nr 5** do Polityki Bezpieczeństwa Informacji;
    c) każdy pracownik zobowiązał się do zachowania danych osobowych przetwarzanych w kancelarii w tajemnicy. Oświadczenie i zobowiązanie osoby przetwarzającej dane osobowe do zachowania tajemnicy stanowi **Załącznik nr 6** do Polityki Bezpieczeństwa Informacji.

V. OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

1. Obszar, w którym przetwarzane są dane osobowe w Kancelarii Forystek & Partnerzy Adwokaci i Radcowie Prawni obejmuje pomieszczenie biurowe kancelarii zlokalizowane w siedzibie Kancelarii przy ul. Grzegórzeckiej 21 (31-532 Kraków), pomieszczenie biurowe oddziału Kancelarii zlokalizowane przy ul. Grzybowskiej 12/14 (00-132 Warszawa) oraz pomieszczenie biurowe oddziału Kancelarii zlokalizowane przy ul. Warszawskiej 18 (35-205 Rzeszów).
2. Dodatkowo obszar, w którym przetwarzane są dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym w ust. 1 powyżej.

VI. 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. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych zostały określone w **Załączniku nr 2** do Polityki Bezpieczeństwa Informacji. Dodatkowo, celem zapewnienia zgodności z prawem procesu przetwarzania danych osobowych zapewnia się co następuje:

- Przetwarzanie i przechowywanie danych osobowych odbywa się w pomieszczeniach biurowych o ograniczonym i kontrolowanym dostępie;
- Zabezpieczenie materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym. dane osobowe zawarte w zbiorze w formie papierowej muszą być przechowywane w pokojach zamykanych na klucz. Klucze należy przechowywać w sposób bezpieczny, bez możliwości dostępu do nich osób nieuprawnionych;
- Wyposażenie budynku w którym przetwarzane są dane osobowe we wzmocnione drzwi, odpowiednio zabezpieczone okna, meble, zamknięcia, instalacje alarmowe i przeciwpożarowe;
- Odpowiednie do zagrożeń wyposażenie i zabezpieczenie pomieszczeń specjalnych takich jak serwerownia i archiwum;
- Stosowanie mechanizmów kontroli dostępu fizycznego do systemów i zasobów chronionych;
- Zastosowanie odpowiednich i regularnie aktualizowanych narzędzi ochronnych w postaci programów antywirusowych, ochronę przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń;
- Regularne tworzenie kopii zapasowych zbiorów danych osobowych przetwarzanych w systemach informatycznych;
- Zastosowanie ochrony zasilania przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
- Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe w sposób bezpieczny uniemożliwiający odczytanie zawartej w nich treści, w szczególności z wykorzystaniem niszczarek.

3. Administrator dokonuje regularnej analizy skuteczności stosowanych środków technicznych i organizacyjnych.

VII. NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

1. Osobą odpowiedzialną za bezpieczeństwo danych osobowych jest Administrator.
2. W przypadku naruszenia bezpieczeństwa danych osobowych, osoba stwierdzająca naruszenie obowiązana jest niezwłocznie zawiadomić Administratora o naruszeniu.
3. W przypadku stwierdzenia naruszenia zasad ochrony danych osobowych Administrator podejmuje następujące działania:

- uniemożliwia lub podejmuje działania mające na celu uniemożliwienie dalszego trwania naruszeń;
- zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić źródło ustalenia przyczyny naruszenia;
- ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających;
- dokonuje oceny czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych;
- sporządza raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wniosku ze zdarzenia – wzór raportu z naruszenia ochrony danych stanowi **Załącznik nr 8** do Polityki Bezpieczeństwa Informacji .

4. Administrator prowadzi rejestr naruszeń ochrony danych osobowych zgodnie z **Załącznikiem nr 9** do Polityki Bezpieczeństwa Informacji.
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.
6. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

VIII. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator 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. Administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi wskazane przez RODO i chroniło prawa osób, których dane dotyczą.
3. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.
4. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej pisemnej zgody administratora.

IX. PRZEKAZYWANIE DANYCH DO PAŃSTWA TRZECIEGO

1. Administrator nie będzie przekazywał danych osobowych do państwa trzeciego, tj. państwa nienależącego do Europejskiego Obszaru Gospodarczego, poza sytuacjami w których przekazywanie następuje na wniosek osoby, której dane dotyczą.

X. POSTANOWIENIA KOŃCOWE

1. Polityka bezpieczeństwa Informacji jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.
2. 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.
3. Integralną część niniejszej Polityki Bezpieczeństwa Informacji stanowią następujące Załączniki:

- **Załącznik nr 1** – Instrukcja zarządzania systemem informatycznym;
- **Załącznik nr 2** – Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalnością przetwarzanych danych osobowych;
- **Załącznik nr 3** – Polityka czystego biurka;
- **Załącznik nr 4** – Rejestr Czynności Przetwarzania;
- **Załącznik nr 5** – Upoważnienie do przetwarzania danych osobowych;
- **Załącznik nr 6** – Oświadczenie o zapoznaniu z zasadami ochrony danych osobowych;
- **Załącznik nr 7** – Rejestr żądań osoby, której dane są przetwarzane;
- **Załącznik nr 8** – Raport z naruszenia ochrony danych osobowych
- **Załącznik nr 9** – Rejestr naruszeń ochrony danych osobowych

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

W

KANCELARII FORYSTEK I PARTNERZY ADWOKACI I RADCOWIE PRAWNI SPÓŁKA PARTNERSKA

KRAKÓW, DNIA 24 MAJA 2018 ROKU

I.

POSTANOWIENIA OGÓLNE

1. Niniejsza instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (dalej: „Instrukcja") przyjęta została w celu zapewnienia zgodności przetwarzania danych osobowych w systemach informatycznych Kancelarii Forystek & Partnerzy Adwokaci i Radcowie Prawni 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).
2. Administratorem danych osobowych jest kancelaria Forystek & Partnerzy Adwokaci i Radcowie Prawni Spółka Partnerska z siedzibą w Krakowie, ul. Grzegórzecka 21 (31-532 Kraków), wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie, XI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000179150, NIP: 6772219730.

II.
PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

1. Za bezpieczeństwo danych osobowych w systemie informatycznym Kancelarii Forystek & Partnerzy Adwokaci i Radcowie Prawni i za właściwy nadzór nad bezpieczeństwem danych w systemie informatycznym Kancelarii odpowiedzialny jest Administrator.
2. Do obsługi systemu informatycznego Kancelarii oraz urządzeń wchodzących w jego skład, a służących do przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania danych wydane przez Administratora.
3. Upoważnienie do przetwarzania danych osobowych nadawane jest w związku z wykonywaniem przez upoważnioną osobę obowiązków lub zadań związanych z przetwarzaniem danych osobowych na rzecz Administratora.
4. Po udzieleniu upoważnienia do przetwarzania danych osobowych w systemie informatycznym nadaje się upoważnionej osobie identyfikator użytkownika. Z chwilą nadania użytkownikowi identyfikatora, osoba ta może uzyskać dostęp do systemów informatycznych w zakresie odpowiednim do udzielonego upoważnienia.
5. Dla każdego użytkownika systemu informatycznego ustalony jest odrębny identyfikator i hasło, które są nadawane przez Administratora.
6. Identyfikator użytkownika nie może być zmieniany. Po wyrejestrowaniu użytkownika z systemu informatycznego identyfikator nie może być przydzielony innej osobie.

7. Identyfikator osoby, która utraciła uprawnienia do dostępu do danych osobowych zostaje niezwłocznie wyrejestrowany z systemu informatycznego, w którym dane osobowe są przetwarzane. Hasło dostępu takiej osoby zostaje unieważnione i zostają podjęte inne działania wyłączające dalszy dostęp tej osoby do danych osobowych.

III.
METODY I ŚRODKI UWIERZYTELNIANIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. Do uwierzytelnienia użytkownika na poziomie dostępu do systemu operacyjnego stosuje się hasło oraz identyfikator użytkownika.
2. Minimalna długość hasła przydzielonego użytkownikowi wynosi 10 znaków alfanumerycznych i znaków specjalnych. Hasło ma mieć charakter unikalny, nie może mieć jednakowego brzmienia jak identyfikator. Hasło nie może składać się z identycznych znaków lub ciągu znaków klawiatury.
3. W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie Administratora.
4. Używanie identyfikatora lub hasła drugiej osoby jest zabronione.
5. Hasła użytkowników umożliwiające dostęp do systemu informatycznego utrzymuje się w tajemnicy również po upływie ich ważności.

IV.
PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZ UŻYTKOWNIKÓW SYSTEMU

1. Pracownik przed uruchomieniem stacji roboczej powinien sprawdzić, czy nie ma widocznych oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, pracownik zobowiązany jest do niezwłocznego powiadomienia o nich Administratora.
2. Po uruchomieniu stacji roboczej pracownik loguje się do systemu przy pomocy identyfikatora użytkownika oraz hasła.
3. Hasło w trakcie wpisywania nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy również po utracie jego ważności.
4. W trakcie pracy przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane jakiekolwiek 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).
6. Zakończenie pracy w systemie powinno zostać poprzedzone sporządzeniem, w miarę potrzeb, kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych, płyt CD, pendrive i innych nośników zawierających dane osobowe.
7. Zakończenie pracy w systemie następuje poprzez wylogowanie się z tego systemu

V.
SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH

1. Kopie zapasowe powinny być kontrolowane przez Administratora, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.
2. Nośniki z kopiami archiwalnymi powinny być zabezpieczone przed dostępem do nich osób nieupoważnionych, a także przed zniszczeniem oraz kradzieżą.
3. Urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar, w którym są one przetwarzane, zabezpiecza się w sposób zapewniający poufność i integralność danych.
4. Nośniki informacji, kopie zapasowe, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
5. Nośników z danymi zarchiwizowanymi nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych, które są używane na bieżąco.
6. Kopie, które są już nieprzydatne, należy zniszczyć fizycznie lub stosując wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane kasowane.
7. W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

VI.
SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ WIRUSÓW KOMPUTEROWYCH, NIEUPRAWNIONYM DOSTĘPEM ORAZ AWARIAMI ZASILANIA

1. System informatyczny jest zabezpieczony przed działaniem złośliwego oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu do systemu oraz przed działaniami inicjowanymi z sieci zewnętrznej. Zabezpieczenie obejmuje:
   a) w przypadku stacji roboczych: system antywirusowy, firewall oraz szyfrowanie nośników danych;
   b) w przypadku sieci wewnętrznej: system antywirusowy oraz firewall;
   c) w przypadku poczty e-mail: szyfrowanie danych, system antywirusowy oraz antyspamowy.
2. Użytkowany system jest automatycznie skanowany pod kątem zagrożeń.
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;
   c) w razie potrzeby zawiadomić Administratora.
5. 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.

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 i 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, przed rozpoczęciem tych czynności dane i programy znajdujące się w systemie powinny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą,
   b) 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,
   c) w przypadku prac serwisowych dokonywanych przez podmiot zewnętrzny, wymagających dostępu do danych osobowych, z podmiotem takim powinny zostać zawarte stosowne umowy powierzenia danych osobowych.

ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

W niniejszym dokumencie zostały przedstawione możliwe zagrożenia, których zidentyfikowanie może mieć wpływ na bezpieczeństwo danych osobowych przetwarzanych w ramach Kancelarii Forystek i Partnerzy Adwokaci i Radcowie Prawni.

I. POUFNOŚĆ DANYCH

Wyróżnia się następujące zagrożenia dla poufności danych:

- Przebywanie nieuprawnionych osób w obszarze przetwarzania danych osobowych;
- Wynoszenie danych osobowych poza obszar ich przetwarzania;
- Wysyłanie plików zawierających dane osobowe za pomocą poczty elektronicznej;
- Nieuwaga, lekkomyślność osób przetwarzających dane osobowe;
- Przetwarzanie danych osobowych przez osoby nieposiadające upoważnień – ujawnienie danych;
- Zbieranie danych osobowych przez osobę nieuprawnioną;
- Brak kontroli i ewidencjonowania elektronicznych nośników zawierających dane osobowe;
- Kompromitacja kluczy szyfrujących odpowiedzialnych za bezpieczną komunikację;
- Istnienie luki w oprogramowaniu pozwalającej na przechwycenie komunikacji w trybie nienadzorowanym;
- Działanie hakerów;
- Kradzież lub rabunek danych znajdujących się na nośnikach.

W celu zapewnienia przetwarzanym danym osobowym atrybutów **poufności** stosuje się następujące zabezpieczenia:

- dostęp do pomieszczenia Kancelarii możliwy jest wyłącznie dla upoważnionych osób posiadających kartę magnetyczną umożliwiającą wejście na teren Kancelarii. Osoby trzecie wchodzące na teren Kancelarii każdorazowo legitymowane są przez pracownika ochrony;
- zbiory danych osobowych w formie papierowej są przechowywane w pomieszczeniach zamykanych na klucz;
- obowiązuje zakaz udzielania informacji dotyczących danych osobowych na podstawie prośby o takie dane w formie zapytania telefonicznego, za wyjątkiem spraw związanych z wykonywaniem obowiązków służbowych;
- niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe w sposób uniemożliwiający odczytanie zawartej w nich treści tylko z wykorzystaniem niszczarek do papieru i w uzasadnionych przypadkach płyt CD / DVD;
- przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne jedynie w obecności osoby upoważnionej do przetwarzania danych osobowych.
- przetwarzanie danych odbywa się zgodnie z zasadami „czystego biurka" i „czystego ekranu";
- w przypadku zawieszenia pracy z systemem informatycznym w związku z tymczasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest do: zablokowania dostępu do użytkowanego systemu komputerowego, w tym również do informacji prezentowanych na jego wyświetlaczu;
- zastosowano rozwiązanie zabezpieczające stacje robocze przed zagrożeniami ze strony złośliwych aplikacji;
- sieć lokalna jest zabezpieczona w punkcie styku z siecią Internet sprzętowym firewallem;
- udostępnianie danych wyłącznie z wydzielonych stanowisk za zgodą przełożonych;
- zastosowano zabezpieczone hasłem wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika;
- dostęp do systemu oraz wrażliwych funkcji poprzez zdublowane uwierzytelnianie użytkowników do systemu operacyjnego oraz identyfikatora i hasła do wykorzystywanej aplikacji (przy użyciu 8 znakowego hasła alfanumerycznego);
- osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do tych danych są szkolone w zakresie obwiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych. Osoby te są zobowiązane do podpisania stosownego oświadczenia;

- do danych osobowych mają dostęp jedynie osoby posiadające upoważnienie nadane przez Administratora;
- osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy;
- tymczasowe wydruki z danymi osobowymi są po ustaniu ich przydatności niszczone w niszczarce;
- korespondencja w zakresie procedur kadrowo-płacowych prowadzona jest za pomocą listów poleconych;
- zapewniono klauzule poufności z wszystkimi podmiotami zewnętrznymi mającymi dostęp do danych osobowych Kancelarii, chyba że obowiązek zachowania poufności wynika z zasad tajemnicy zawodowej;

II. DOSTĘPNOŚĆ I INTEGRALNOŚĆ DANYCH

Wyróżnia się następujące zagrożenia dla dostępności i integralności danych:

- Przypadkowe lub celowe uszkodzenie systemów i aplikacji informatycznych;
- Zamierzone zniszczenie aktywów;
- Fałszerstwo;
- Awaria sprzętu sieciowego;
- Przypadkowe lub celowe uszkodzenie, utrata, zniszczenie, modyfikacja danych osobowych;
- Ataki pochodzące z sieci publicznej;
- Działanie szkodliwego oprogramowania;
- Nieobecność kluczowych pracowników;
- Klęski żywiołowe;
- Wandalizm;
- Ataki terrorystyczne;
- Trwała lub czasowa utrata dostępu do zasobów informatycznych;
- Przerwy w dopływie energii elektrycznej oraz nieprawidłowe działanie urządzeń podtrzymujących zasilanie;
- Przeciążenie lub awarie sprzętu sieciowego;
- Uszkodzenie lub nieautoryzowana modyfikacja danych osobowych;

- Uszkodzenie, celowe lub przypadkowe oprogramowania aplikacyjnego lub użytkowego służącego do przetwarzania danych osobowych;
- Brak możliwości uruchomienia łącza zapasowego w przypadku uszkodzenia łącza podstawowego;
- Niedostosowanie przepustowości łącza do aktualnej liczby użytkowników systemu.

W celu zapewnienia przetwarzanym danym osobowym atrybutów **dostępności i integralności** stosuje się następujące zabezpieczenia:

- stosowanie haseł z odpowiednią siłą i częstotliwością zmiany;
- wykonywanie kopii zapasowych danych i programów oraz bezpieczny sposób ich przechowywania;
- niektóre systemy służące do przetwarzania danych osobowych w sieci posiadają architekturę klient-serwer, wobec czego wszystkie informacje przechowywane są na serwerze, przez co możliwe jest lepsze zabezpieczenie danych. Serwer decyduje, kto ma prawo do odczytywania, kopiowania i zmiany danych;
- komputery przenośne i elektroniczne nośniki informacji użytkowane w Spółce zawierające dane osobowe, nie są transportowane, przechowywane, użytkowane i przekazywane poza obszar, o którym mowa w § 4 pkt. 1 Rozporządzenia MSWiA;
- stosowanie zasad wykonywania okresowych przeglądów systemu informatycznego;
- opracowano i wdrożono Instrukcję Zarządzania Systemem Informatycznym, Politykę Bezpieczeństwa Danych Osobowych oraz ewidencję osób upoważnionych do przetwarzania danych osobowych;
- zapewnia się bezpieczeństwo nośników informacji zawierających dane osobowe w przypadku, gdy zachodzi konieczność naprawy sprzętu, w którym te nośniki są zamontowane (wymontowanie w przypadku naprawy poza siedzibą Spółki lub nadzór nad serwisem w siedzibie Spółki);
- zastosowano system ochrony ciągłości zasilania, zmniejszający ryzyko utraty danych znajdujących się aktualnie w pamięci operacyjnej serwerów, a nawet uszkodzenia urządzeń pamięci masowej.

III. ROZLICZALNOŚĆ DANYCH

Wyróżnia się następujące zagrożenia dla rozliczalności danych:

- Nieprzydzielenie użytkownikom systemu informatycznego unikalnego identyfikatora w jego obrębie;

- Brak adekwatnych do wymagań prawa mechanizmów kontroli dostępu do danych;
- Niewłaściwa administracja systemem informatycznym;
- Niewłaściwa konfiguracja systemu informatycznego;
- Brak księgi administratora;
- Zbyt duże uprawnienia użytkowników systemu informatycznego;
- Zniszczenie lub sfałszowanie logów systemowych.

W celu zapewnienia przetwarzanym danym osobowym atrybutów **rozliczalności** stosuje się następujące zabezpieczenia:

- stosowanie procedury rozpoczęcia, zawieszenia, zakończenia pracy przez użytkownika;
- stosowane są zasady postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych;
- system informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu;
- wprowadzono mechanizmy autoryzacji odpowiednio zabezpieczone przed dostępem osób trzecich;
- identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie.

POLITYKA CZYSTEGO BIURKA

1. Niniejsza polityka czystego biurka obowiązuje wszystkich pracowników Kancelarii Forystek & Partnerzy Adwokaci i Radcowie Prawni.
2. Za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, powołania, wyboru, mianowania lub spółdzielczej umowy o pracę, a także osobę fizyczną wykonującą pracę na innej podstawie niż stosunek pracy, jak również osobę prowadzącą jednoosobową działalność gospodarczą, współpracującą z Kancelarią.
3. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań.
4. Pracownik zobowiązany jest do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce.
5. Na biurku nie mogą znajdować się napoje w pojemnikach grożących rozlaniem płynu.
6. Monitory ekranów powinny być ustawione w sposób uniemożliwiający klientom i innym osobom trzecim wgląd w dane osobowe wyświetlane na ekranie.
7. Każdorazowe odejście od stanowiska pracy powinno zostać poprzedzone wylogowaniem się lub zablokowaniem dostępu do systemu tak, aby niemożliwe było uzyskanie nieautoryzowanego dostępu do systemu.
8. Po zakończonej pracy na biurku mogą znajdować się jedynie komputer, telefon i przybory biurowe, takie jak: zszywacz, dziurkacz, długopis, itp.

REJESTR CZYNNOŚCI PRZETWARZANIA

Nazwa czynności przetwarzania		
Cel przetwarzania		

Kategorie osób		
Kategorie danych		
Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)		
Nazwa współadministratora i dane kontaktowe (jeżeli dotyczy)		
Nazwa podmiotu przetwarzającego i dane kontaktowe (jeżeli dotyczy)		
Kategorie odbiorców (innych niż podmiot przetwarzający)		
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)		
Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)		
W przypadku transferu do kraju trzeciego – dokumentacja odpowiednich zabezpieczeń		

Nazwa czynności przetwarzania		
Cel przetwarzania		
Kategorie osób		
Kategorie danych		

Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)		
Nazwa współadministratora i dane kontaktowe (jeżeli dotyczy)		
Nazwa podmiotu przetwarzającego i dane kontaktowe (jeżeli dotyczy)		
Kategorie odbiorców (innych niż podmiot przetwarzający)		
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)		
Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)		
W przypadku transferu do kraju trzeciego – dokumentacja odpowiednich zabezpieczeń		

Nazwa czynności przetwarzania		
Cel przetwarzania		
Kategorie osób		
Kategorie danych		
Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe)		

Nazwa współadministratora i dane kontaktowe (jeżeli dotyczy)		
Nazwa podmiotu przetwarzającego i dane kontaktowe (jeżeli dotyczy)		
Kategorie odbiorców (innych niż podmiot przetwarzający)		
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)		
Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)		
W przypadku transferu do kraju trzeciego – dokumentacja odpowiednich zabezpieczeń		

Kraków , dnia _____ r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając w imieniu Forystek i Partnerzy Adwokaci i Radcowie Prawni spółka partnerska z siedzibą w Krakowie, ul. Grzegórzecka 21 (31-532 Kraków), wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Krakowa-Śródmieścia w Krakowie, XI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000179150 (dalej: „Kancelaria"), niniejszym upoważniam:

Panią/Pana _____

do przetwarzania danych osobowych w Kancelarii w zakresie danych przetwarzanych na nośnikach papierowych, w systemie informatycznym oraz danych osobowych objętych zbiorem.

Zakres upoważnienia obejmuje:

1. Dostęp do strefy przetwarzania danych osobowych i przebywania w niej samodzielnie;
2. Przetwarzania danych osobowych w zbiorze danych osobowych w zakresie:
   a) Wyszukiwanie danych;
   b) Przeglądanie danych
   c) Usuwania danych;
   d) Dzielenia danych;
   e) Przenoszenia danych;
   f) Modyfikowania danych;

W celu ochrony danych osobowych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, osoba upoważniona jest zobowiązana do przestrzegania właściwych przepisów o ochronie danych osobowych, jak również postanowień Polityki Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemem Informatycznym obowiązujących w Kancelarii, w tym w szczególności, do:

1. dokonywania regularnych zmian hasła dostępowego do konta i innych haseł, zgodnie z Polityką haseł i uwierzytelniania w systemach Spółki;
2. nieujawniania osobom postronnym haseł oraz szczegółów dotyczących działania systemu informatycznego Spółki.

Upoważnienie obowiązuje w okresie współpracy z Kancelarią.

_____

Podpis Administratora

Oświadczam, że otrzymałem niniejsze upoważnienie, zrozumiałem jego treść i w pełni akceptuję zakres moich obowiązków służbowych dotyczących przetwarzania danych osobowych powierzonych mi przez Spółkę.

_____

Podpis osoby upoważnionej

Kraków , dnia _____ r.

_____

imię i nazwisko osoby upoważnionej

OŚWIADCZENIE O ZAPOZNANIU Z ZASADAMI OCHRONY DANYCH OSOBOWYCH

Oświadczam, że w związku z wykonywaniem przeze mnie czynności na rzecz Forystek i Partnerzy Adwokaci i Radcowie Prawni Spółka Partnerska (Administrator) i upoważnieniem mnie przez Administratora do przetwarzania danych osobowych – zostałem/łam zapoznany/a ze stosownymi przepisami i standardami ochrony danych osobowych obowiązującymi w Kancelarii.

Niniejszym, zobowiązuję się do przestrzegania:

- Przepisów o ochronie tajemnicy zawodowej;
- 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;
- Polityki Bezpieczeństwa informacji w Forystek i Partnerzy i Radcowie Prawni Spółka Partnerska;
- Instrukcji zarządzania systemem Informatycznym w Forystek i Partnerzy i Radcowie Prawni Spółka Partnerska;

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

_____

[podpis współpracownika]

REJESTR ŻĄDAŃ OSOBY, KTÓREJ DANE SĄ PRZETWARZANE

I. Żądanie

1. Data zgłoszenia żądania:

   ……...

2. Zgłaszający żądanie:

   ……...

3. Treść żądania:

   ……...

II. Obsługa żądania

1. Pracownik obsługujący żądanie:

   ……...

2. Czy dane zgłaszającego żądanie są przetwarzane przez administratora danych:

   ……...

3. Czy dane zgłaszającego żądanie zostały powierzone (komu, kiedy):

   ……...

4. Podjęte czynności:

   Osoba podejmująca czynności: ……

   a) Czynność I

   - Opis czynności:

   ……...

- Data dokonania czynności:

……...

b) Czynność II

- Opis czynności:

……...

- Data dokonania czynności:

……...

…….

Podpis Administratora

RAPORT Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Data ……. Godzina ……

2. Zawiadamiający o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe):

   ……..

3. Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

   ……

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

   ……

5. Podjęte działania:

   ……

6. Wstępna ocena przyczyn wystąpienia naruszenia:

   …….

7. Postępowanie wyjaśniające i naprawcze:

   …….

…….……

(data i podpis Administratora)

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH					
Rodzaj naruszenia	Obowiązek zgłoszenia organowi nadzorczemu	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze
	Tak / Nie	**Tak / Nie**			
	Tak / Nie	**Tak / Nie**			
	Tak / Nie	**Tak / Nie**			
	Tak / Nie	**Tak / Nie**			