POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w Okręgowej Izbie Radców Prawnych w Toruniu

Toruń,

24 września 2018 r.

Niniejsza *Polityka bezpieczeństwa danych osobowych*, zwana dalej Polityką, została sporządzona w celu potwierdzenia, że dane osobowe gromadzone w Okręgowej Izbie Radców Prawnych w Toruniu (dalej zwana OIRP Toruń) są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w OIRP Toruń, 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) oraz ustawą o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. 2018 poz. 1000). Niniejsza Polityka stanowi jeden ze środków organizacyjnych, mających na celu zadbanie, żeby przetwarzanie danych osobowych odbywało się zgodnie zobowiązującymi przepisami prawa. Celem Polityki jest również opisanie zasad dotyczących zapewnienia bezpieczeństwa danych i informacji przetwarzanych w OIRP Toruń, w tym zasad ochrony przetwarzanych danych osobowych.

Utrzymanie bezpieczeństwa przetwarzanych danych osobowych rozumiane jest jako zapewnienie ich poufności, integralności, dostępności i rozliczalności, przy czym:

1) **Poufność informacji** – rozumiana jest, jako zapewnienie, że tylko osoby uprawnione mają dostęp do informacji,
2) **Integralność informacji** – rozumiana jest jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
3) **Dostępność informacji** – rozumiane jest, jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
4) **Rozliczalność informacji** – rozumiana jest jako zapewnienie możliwości przypisania w sposób jednoznaczny zrealizowanej czynności do określonego podmiotu.

Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów niniejszego dokumentu powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

Niniejsza procedura dotyczy całego personelu OIRP Toruń. Polityka ma zastosowanie do wszystkich danych osobowych przetwarzanych w OIRP Toruń, w ramach procesów przetwarzania danych osobowych.

Obowiązek ochrony danych osobowych przetwarzanych w OIRP Toruń dotyczy wszystkich osób, które mają do nich dostęp bez względu na zajmowane stanowisko, oraz miejsce wykonywania pracy, jak również charakter stosunku pracy.

Każda osoba, która ma dostęp do danych osobowych, będzie mogła je przetwarzać wyłącznie na podstawie otrzymanego upoważnienia.

Osoby mające dostęp do danych osobowych są zobowiązane do zapoznania się z Polityką i innymi powiązanymi z nią dokumentami oraz stosowania zawartych w nich regulacji.

Polityka zachowuje zgodność z innymi wewnętrznymi regulacjami z obszaru bezpieczeństwa informacji i systemów informatycznych obowiązującymi w OIRP Toruń.

Nadzór nad opracowaniem i aktualizacją Polityki sprawuje Prezydium OIRP w Toruniu. Polityka powinna być poddawana bieżącej aktualizacji, ale nie rzadziej niż raz do roku

Definicje:

1. **Administrator Danych-** Okręgowa Izba Radców Prawnych w Toruniu.

2. **Dane osobowe** – oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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;

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,
5. **Zbiór danych** – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów**,**
6. **Przetwarzanie danych** – oznacza operację lub zestaw operacji wykonywanych na Danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
7. **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,
8. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie Użytkownikowi w razie przetwarzania danych osobowych w takim systemie,
9. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości Użytkownika,
10. **Pracownik** – osoba zatrudniona w OIRP Toruń, niezależnie od podstawy prawnej zatrudnienia (np. umowa o pracę, umowa o świadczenie usług, umowa o dzieło)
11. **Prezydium Rady OIRP** - organ wykonawczy rady OIRP Toruń.
12. **Inspektor Ochrony Danych (IOD)** - wyznaczona przez OIRP Toruń osoba odpowiedzialna za monitorowanie zgodności działań OIRP z obowiązującymi przepisami o ochronie danych osobowych, e-mail: oirp@torun.oirp.pl.
13. **Administrator Systemu Informatycznego** – osoba administrująca systemem służącym do przetwarzania i przechowywania informacji podlegającej ochronie w OIRP Toruń, w tym danych osobowych
14. **Podmiot Przetwarzający (Procesor)** – osoba fizyczna lub prawna, która przetwarza dane w imieniu Administratora Danych; na podstawie umowy powierzenia przetwarzania danych, będącej elementem umowy o świadczenie usług na rzecz OIRP.
15. **Rozporządzenie/RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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).

I. Postanowienia ogólne.

1. Ustala się, iż w Okręgowej Izbie Radców Prawnych w Toruniu, stosuje się Politykę niezależnie od formy przetwarzania Danych Osobowych (przetwarzanie tradycyjnie papierowo w zbiorach ewidencyjnych oraz w systemach informatycznych).
2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych, a także osobom, którym mają zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.
4. Dane osobowe przetwarzane w OIRP w Toruniu objęte są tajemnicą.
5. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
   a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
   b) kontrolę i nadzór nad Przetwarzaniem danych osobowych,
   c) monitorowanie zastosowanych środków ochrony.
6. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania Użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików, oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
7. Administrator Danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą Polityką, oraz odpowiednimi przepisami prawa.

II. **Dane osobowe przetwarzane u Administratora Danych**

1. Jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.
2. W przypadku planowania nowych czynności przetwarzania, a także dla wszystkich obecnych, Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
3. Administrator danych prowadzi rejestr czynności przetwarzania. Wzór rejestru czynności przetwarzania stanowi załącznik nr 1 do niniejszej polityki.

4. Administrator Danych ma obowiązek:

a) Zapewnienia środków technicznych i organizacyjnych do ochrony przetwarzanych danych osobowych, odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, w szczególności zabezpieczeniem danych przed:

- udostępnieniem osobom nieupoważnionym,
- zabraniem przez osobę nieuprawnioną,
- zmianą, utratą, uszkodzeniem lub zniszczeniem.

b) Zapewnienie legalności przetwarzania danych osobowych,

c) Wyznaczenie IOD nadzorującego przestrzeganie zasad ochrony danych osobowych.

d) Wyznaczenie ASI odpowiedzialnego za bezpieczeństwo systemów informatycznych służących do przetwarzania danych osobowych.

e) Dopuszczanie do przetwarzania danych wyłącznie osoby przeszkolonej i posiadającej upoważnienie, oraz wydawanie i zarządzanie upoważnieniami.

f) Nadzorowanie i dbanie o zgodne z prawem przekazywanie danych osobowych (udostępnianie i powierzanie).

g) Respektowanie praw osób, których dane dotyczą, a w szczególności prawa do uzyskania informacji.

h) W przypadku pozyskania danych nie od osoby, której one dotyczą - zapewnienie, ze wobec osób, których dane dotyczą wykonano tzw. obowiązek informacyjny zgodnie z art. 14 Rozporządzenia wraz ze wskazaniem im praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu);

i) Respektowanie praw osób, których dane dotyczą w zakresie: dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania, przenoszenia danych, cofnięcia zgody na przetwarzanie danych osobowych, wniesienia skargi do organu nadzorczego.

j) Zapewnienie ochrony danych w przypadku powierzenia przetwarzania danych osobowych w postaci umów powierzenia z podmiotami przetwarzającymi (zawartymi zgodnie z art. 28 RODO).

k) Zapewnienie, że dane są przetwarzane na podstawie i w granicach umowy powierzenia do przetwarzania danych osobowych oraz zgodnych z prawem instrukcjami administratora danych.

l) Przeprowadzanie regularnych wewnętrznych audytów przestrzegania przepisów dotyczących ochrony danych osobowych.

III. **Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem danych osobowych.**

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Polityką, oraz innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych w OIRP Toruń.

2. Wszystkie dane osobowe w Okręgowej Izbie Radców Prawnych są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
   a) każdorazowo 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 nie-zbędny 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 a nadto do celów, do których zostały zebrane, 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. Administrator danych 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).
4. 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 udostępniania danych osobom lub pod-miotom 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 nie-uprawnione kopiowanie Danych osobowych;
   g) naruszenie praw osób, których dane są przetwarzane.
5. W przypadku stwierdzenia okoliczności powodujących naruszenie zasad ochrony danych osobowych Użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych,
6. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) należy dbanie o to, aby:
   a)pracownicy/współpracownicy 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" – wzór Upoważnienia stanowi załącznik nr 2 do niniejszej Polityki Bezpieczeństwa,
   c) każdy pracownik zobowiązał się do zachowania danych osobowych przetwarzanych w OIRP Toruń w tajemnicy. Stosowne oświadczenie zostało zawarte w Upoważnieniu stanowiącym Załącznik nr 2 do niniejszej Polityki Bezpieczeństwa,
7. Pracownicy zobowiązani są do:
   a) ścisłego przestrzegania zakresu nadanego upoważnienia;
   b) przetwarzania i ochrony danych osobowych zgodnie z przepisami;
   c) zachowania w tajemnicy danych osobowych, oraz ustalonych sposobów w zakresie ich zabezpieczania;

d) niezwłocznego zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.

IV. Obszar przetwarzania danych osobowych

1. Obszar w którym przetwarzane są Dane osobowe: w siedzibie Okręgowej Izby Radców Prawnych w Toruniu zlokalizowane w Toruniu (87-100) ul. Chełmińska 16, oraz w Ośrodku Szkolenia Aplikantów Radcowskich ul. Gdańska 4a, 87-100 Toruń.
2. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią komputery przenośne, oraz inne nośniki danych znajdujące się poza obszarem wskazanym powyżej.

V. 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 obejmują:
   a) Ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie dla osób do tego upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych osobowych jedynie wraz z osobą upoważnioną.
   b) Zabezpieczanie i zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w pkt IV powyżej na czas nieobecności upoważnionych pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich.
   c) Wykorzystanie zamykanych szafek i sejfów celem 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) Wykonywanie kopii awaryjnych danych na specjalnie do tego przeznaczony nośnik,
   g) Ochronę sprzętu komputerowego wykorzystywanego u administratora przed złośliwym oprogramowaniem.
   h) Zabezpieczenie dostępu do urządzeń OIRP Toruń przy pomocy haseł dostępu.
   i) Wykorzystanie szyfrowania danych przy ich transmisji.

VI. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator Danych dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza taki fakt naruszenia zasad ochrony danych organowi nadzorczemu, bez zbędnej zwłoki
   – jeżeli jest to możliwe, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Wzór zgłoszenia określa załącznik nr 3 do niniejszej polityki.
3. W sytuacji uznania, iż naruszenie praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.
4. Sprzęt komputerowy, zewnętrzne nośniki danych, dokumentacja papierowa nie są wynoszone poza siedzibę OIRP, poza osobami uprawnionymi. Zabrania się wynoszenia na zewnątrz OIRP zewnętrznych nośników danych (w tym wymienne twarde dyski, USB, płyty CD/DVD, karty pamięci) czy dokumentacji papierowej z zapisanymi danymi osobowymi, bez zgody Prezydium Rady. W przypadku wynoszenia poza siedzibę OIRP służbowego sprzętu przenośnego (laptopy, tablety, smartfony, zewnętrzne nośniki danych) oraz dokumentacji papierowej przez osoby upoważnione przez Prezydium OIRP obowiązują następujące zasady:
   1) niepozostawianie sprzętu w miejscach publicznych bez nadzoru,
   2) przewożenie laptopów jako bagaż podręczny i maskowanie ich podczas podróży,

3) nieudostępnianie sprzętu osobom trzecim,
4) przestrzeganie instrukcji producenta dotyczącego ochrony sprzętu np. ochrony przed silnym polem elektromagnetycznym,
5) stosowanie odpowiednich zabezpieczeń, niezbędnych podczas pracy w domu (zamykanie szafek, polityka czystego biurka, zabezpieczony dostęp do komputerów),
6) szyfrowanie danych osobowych wynoszonych poza OIRP (hasłowane pliki,),
7) bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach oraz zabezpieczenie przed zgubieniem czy kradzieżą.

5. Czynności służbowe wymagające pracy mobilnej, należy dokonywać wyłącznie na służbowym sprzęcie IT, wyposażonym w mechanizmy zabezpieczające. Zabrania się wykorzystywania prywatnego sprzętu IT (laptopy, tablety, smartfony, itp.) dla celów służbowych za wyjątkiem uzasadnionych przypadków, dla których została wydana zgoda Prezydium OIRP.

VII. 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 radcowskiej tajemnicy zawodowej.
2. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.

VIII. UPOWAŻNIENIA

1. Do przetwarzania danych w OIRP mogą być dopuszczone wyłącznie przeszkolone osoby, którym nadano odpowiednie upoważnienie do przetwarzania danych osobowych oraz które zobowiązały się do zachowania w poufności powierzonych jej danych.
2. IOD odpowiada za proces nadawania/anulowania upoważnień do przetwarzania danych osobowych w zbiorach papierowych oraz systemach informatycznych dla pracowników OIRP oraz wykładowców. Dokument upoważnienia, jest przygotowywany przez wyznaczonego pracownika, na polecenie IOD i przekazywany do podpisu Prezydium OIRP. Podpisany dokument upoważnienia jest przekazywany do IOD i do osoby upoważnianej.
3. Upoważnienia nadawane są indywidulanie, zgodnie z zajmowanym w OIRP stanowiskiem lub realizowanym zadaniem.
4. IOD prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja ma charakter pomocniczy.
5. W celu dopuszczenia do przetwarzania danych osobowych, Administrator Danych nadaje upoważnienie do przetwarzania danych w szczególności następującym kategoriom personelu OIRP: pracownikom, wykładowcom, członkom Rady, sędziom sądu dyscyplinarnego.
6. W sytuacji, w której podmiot zewnętrzny deleguje swoich pracowników lub osoby zatrudnione u niego na podstawie cywilnoprawnych form zatrudnienia do świadczenia usług pod kontrolą i na fizycznym obszarze przetwarzania danych Administratora Danych Osobowych oraz jeżeli nie zachodzi relacja uzasadniająca zawarcie umowy powierzenia, w/w pracownikom lub osobom nadawane jest przez ADO na piśmie upoważnienie do przetwarzania danych osobowych i odbierane jest od nich pisemne oświadczenie o poufności.

IX. ANALIZA RYZYKA/ /OCENA SKUTKÓW DLA OCHRONY DANYCH

1. OIRP jako Administrator Danych posiada dokumentację wskazującą na przeprowadzenie analizy ryzyka związanej ze wszystkimi czynnościami przetwarzania danych osobowych w OIRP. Analiza ryzyka uwzględnia stosowane techniczne i organizacyjne środki zabezpieczenia danych osobowych (Wykaz zabezpieczeń). Analiza ryzyka zawarta jest w Rejestrze Czynności przetwarzania danych.

2. Analiza ryzyka wraz z wykazem zabezpieczeń powyżej jest przeprowadzana okresowo (co najmniej 1 raz w roku,). Za aktualizację analizy ryzyka jest odpowiedzialny IOD we współpracy z ASI i Prezydium Rady OIRP.
3. OIRP jako Administrator Danych dokonuje oceny wykonywanych czynności na danych osobowych pod kątem ochrony danych osobowych, po powzięciu informacji o każdym nowym projekcie podejmowanym w OIRP. **IOD jest obligatoryjnie informowany i włączony w każdy projekt,** celem oceny skutków tego projektu dla ochrony danych osobowych poprzez wykonanie następujących czynności:
   1) Identyfikacja planowanych operacji przetwarzania i celów przetwarzania;
   2) Weryfikacja, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
   3) Ocena ryzyka;
   4) Środki planowane w celu zaradzenia ryzyku, przedstawione w postaci planu postępowania z ryzykiem.

X. 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.

XI. 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 Za-łączniki:

Załącznik nr 1
Rejestr czynności przetwarzania danych osobowych,

Załącznik nr 2
Wzór upoważnienia do przetwarzania danych osobowych,

Załącznik nr 3
Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego.

Załącznik 2. Wzór upoważnienia do przetwarzania danych osobowych

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

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s.1)-dalej RODO - nadaję upoważnienie Pani/Panu:

.....
(imię i nazwisko)

.....
(stanowisko)

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku, tj. uzyskuje Pani/Pan upoważnienie do przetwarzania danych osobowych na poziomie .....

Upoważnienie obejmuje uprawnienie do przetwarzania danych ..... dostępnych w zasobach ....., w okresie zatrudnienia, bez prawa dostępu do informacji o wynagrodzeniach itp.

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, ustawy z dnia [.....] o ochronie danych osobowych, Kodeksu pracy, a także polityką ochrony danych osobowych Pracodawcy.

Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony, przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w [.....].

Okres ważności
od:
do:

.....
podpis osoby uprawnionej
do nadania upoważnienia

Data wygaśnięcia*.....
Odwołano, dnia.....

.....
podpis osoby uprawnionej
do odwołania upoważnienia

*Data rozwiązania stosunku pracy/umowy cywilnoprawnej.

. . . . . , dn. . . . . r.
[m-ce/ data sporządzenia]

Prezes Urzędu Ochrony Danych Osobowych

ZGŁOSZENIE INCYDENTU NARUSZENIA
OCHRONY DANYCH OSOBOWYCH

Działając na podstawie art. 33 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 (ogólne rozporządzenie o ochronie danych), niniejszym zgłaszam zajście incydentu naruszenia ochrony danych osobowych.

Dane Administratora Danych Osobowych
……
Miejsce i dzień naruszenia
…….
Kategoria i przybliżona ilość wpisów, których danych osobowych, których dotyczy naruszenie
……..
Kategoria i przybliżona ilość osób, których dane dotyczą
……..