OŚRODEK TECHNIKI LEŚNEJ
63-200 Jarocin, ul. Prze[illegible] 25
Bank Zachodni WBK S.A. Oddział Jarocin
97 1090 1131 0000 0000 1300 9302
tel. 062/7473582, fax 062/7472933
Nr ident. NIP 617-08-05-354
REGON 250027011

Zarządzenie nr 15 / 2018

Dyrektora Ośrodka Techniki Leśnej w Jarocinie
z dnia 29 maja 2018 roku

w sprawie wdrożenia

POLITYKI BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

w Ośrodku Techniki Leśnej w Jarocinie

Znak spr. KA.0171.1 .2018

Aleksandra Jakrzewska

Od: Aleksandra Jakrzewska <a.jakrzewska@otljarocin.lasy.gov.pl>
Wysłano: czwartek, 18 października 2018 10:32
Do: Bernadeta Błaszczyk (bernadeta.blaszczyk@otljarocin.lasy.gov.pl); Marek Bambrowicz (marek.bambrowicz@otljarocin.lasy.gov.pl); 'piotr.grzybowski@otljarocin.lasy.gov.pl'; Paweł Grzybowski (pawel.grzybowski@otljarocin.lasy.gov.pl); 'Paweł Cuprych (pawel.cuprych@otljarocin.lasy.gov.pl)'; Anna Tokarz (anna.tokarz@otljarocin.lasy.gov.pl); 'Lidia Grygiel'; 'Marika Grzemska'; Andrzej Dudziak (andrzej.dudziak@otljarocin.lasy.gov.pl); Krzysztof Ewiak; Sebastian Nieciąg; 'Czesław Chudak'; krzysztof.brek@otljarocin.lasy.gov.pl; 'Tomasz Papież'; 'Maciej Kolański'; 'Tomasz Oleś'; tomasz.pankowiak@otljarocin.lasy.gov.pl; tomasz.zaradny@otljarocin.lasy.gov.pl; 'Agnieszka Brugger'; 'skp@otljarocin.lasy.gov.pl'
DW: Ryszard Misiek
Temat: Zarz.nr 15.2018 Polityka bezpieczeństaw przetwarzania danych osobowych
Załączniki: Zarz.nr 15.2018 Polityka bezpieczeństaw przetwarzania danych osobowych.pdf

W załączeniu przesyłam Państwu Zarządzenie nr 15/2018 Dyrektora Zakładu w sprawie wdrożenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych.

Pozdrawiam

Aleksandra Jakrzewska
Kierownik Działu Kięgowo-Ekonomicznego
Ośrodek Techniki Leśnej
Ul. Przemysłowa 2D
63-200 Jarocin
Tel. 62 749 80 48
Tel. 602 114 458

Wiadomość jest gotowa do wysłania wraz z następującymi załącznikami (plikami lub linkami):

Zarz.nr 15.2018 Polityka bezpieczeństaw przetwarzania danych osobowych

ROZDZIAŁ I
INFORMACJE WSTĘPNE

1. Polityka Bezpieczeństwa

Politykę bezpieczeństwa należy rozumieć, jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji o danych osobowych wewnątrz organizacji. Polityka jest obowiązującym dokumentem określającym procedury przetwarzania danych osobowych w formie tradycyjnej, jak i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji u Administratora.

2. Zakres informacji objętych Polityką Bezpieczeństwa

Dokument opisuje procedury bezpieczeństwa danych osobowych przetwarzanych w formie tradycyjnej (papierowej) oraz w systemach informatycznych Administratora. Opisane zbiory zasad i procedur określają granice dopuszczalnego zachowania wszystkich użytkowników systemu informatycznego wspomagającego pracę Administratora. Dokument zawiera również opis konsekwencji, jakie mogą ponieść osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

3. Cele utworzenia dokumentacji

Podstawowym celem przygotowania i wdrożenia dokumentu Polityki Bezpieczeństwa jest podniesienie poziomu bezpieczeństwa dokumentów i systemów informatycznych, w których są gromadzone i przetwarzane dane osobowe oraz określenie odpowiedzialności pracowników za prawidłowe działanie tych systemów i bezpieczeństwo przetwarzanych w nim danych.

4. Podstawy prawne opracowania Polityki Bezpieczeństwa

Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

1) 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, zwane dalej „**rozporządzeniem**";

2) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, zwana dalej „**ustawą**".

5. Podstawowe definicje:

1) **Administrator** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
2) **Inspektor Ochrony Danych (IOD)** - osoba powołana przez Administratora w celu zapewnienia stosowania przepisów rozporządzenia oraz dbania o zasady zapisane w niniejszym dokumencie;
3) **Administrator Systemu Informatycznego (ASI)** - rozumie się przez to osobę wyznaczoną przez Administratora do zapewnienia prawidłowego działania infrastruktury informatycznej;

4) **Organ Nadzorczy** - oznacza niezależny organ publiczny ustanowiony zgodnie z art. 51 rozporządzenia;
5) **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;
6) **Przetwarzanie** - 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) **Profilowanie** - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
8) **Naruszenie ochrony danych** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Za naruszenie bezpieczeństwa informacji uważa się również stwierdzone nieprawidłowości w zakresie bezpieczeństwa miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach, pamięciach flash itp. w formie niezabezpieczonej;
9) **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
10) **Odbiorca danych** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

ROZDZIAŁ II
ORGANIZACJA PRZETWARZANIA DANYCH

1. **Administrator:**
   1) Administratorem jest Ośrodek Techniki Leśnej, z siedzibą przy ul. Przemysłowej 2D, 63-200 Jarocin, reprezentowany przez Dyrektora.
   2) Administrator realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:
      a. podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, własnej strukturze organizacyjnej oraz technik zabezpieczania danych osobowych;
      b. wdraża odpowiednie środki techniczne i organizacyjne zabezpieczania danych uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób których dane dotyczą;
      c. upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnym zakresie, odpowiadającym zakresowi jej obowiązków;
      d. może wyznaczyć Inspektora Ochrony Danych oraz określa zakres jego zadań i obowiązków;
      e. może wyznaczyć Administratora Systemu Informatycznego oraz określa zakres jego zadań i obowiązków;
      f. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpieczeństwa przetwarzania danych osobowych.
2. **Inspektor Ochrony Danych:**
   1) Obowiązki Inspektora Ochrony Danych pełni osoba wyznaczona w trybie art. 37 rozporządzenia przez Administratora.
   2) Administrator może każdorazowo odwołać IOD.
   3) Status Inspektor Ochrony Danych:
      a. Administrator zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
      b. Administrator zapewnia IOD zasoby niezbędne do wykonania zadań oraz dostęp do danych osobowych i operacji przetwarzania;
      c. IOD w ramach wykonywania swoich zadań podlega bezpośrednio Administratorowi.
   4) IOD realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:
      a. informuje Administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów o ochronie danych i doradza im w tej sprawie;
      b. monitoruje przestrzeganie rozporządzenia, innych przepisów o ochronie danych oraz polityk Administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
      c. udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitoruje jej wykonanie zgodnie z art. 35 rozporządzenia;
      d. współpracuje z Organem Nadzorczym;
      e. pełnieni funkcję punktu kontaktowego dla Organu Nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36

rozporządzenia, oraz w stosownych przypadkach prowadzi konsultacje we wszelkich innych sprawach.

3. **Administrator Systemu Informatycznego:**
   1) Obowiązki Administratora Systemu Informatycznego pełni osoba/osoby wyznaczone przez Administratora.
   2) Administrator może każdorazowo odwołać ASI.
   3) ASI realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym Administratora, w tym zwłaszcza:
      a. zarządza systemem informatycznym zlokalizowanym u Administratora, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z poziomu administratora;
      b. przeciwdziała dostępowi osób niepowołanych do systemu informatycznego;
      c. zgłasza do zarejestrowania użytkownika w systemie informatycznym w związku z zatrudnieniem pracownika;
      d. przygotowuje do akceptacji uprawnienia w systemach informatycznych upoważnionym użytkownikom zgodnie z dyspozycją;
      e. nadzoruje stosowanie mechanizmów uwierzytelniania użytkowników poprzez kontrolę poprawności użytkowania kont;
      f. w sytuacjach stwierdzenia naruszenia zabezpieczeń systemu informatycznego, informuje Administratora o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia;
      g. podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;
      h. inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych;
      i. informowanie Administratora o konieczności wprowadzenia zmian w Instrukcji zarządzania systemem informatycznym (np. z powodu zmian procedur tworzenia kopii zapasowych lub zmiany zabezpieczeń systemów informatycznych).
4. **Kierownicy działów i samodzielne stanowiska** nadzorują bezpieczeństwo przetwarzania danych osobowych w swoich komórkach/działach poprzez:
   a. zapewnienie prawidłowego przetwarzania danych osobowych;
   b. zapewnienie prawidłowego zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe;
   c. zapewnienie prawidłowego zabezpieczenia danych w formie papierowej;
   d. zapewnienie prawidłowego działania innych zabezpieczeń fizycznych stosowanych u Administratora;
   e. zapewnienie prawidłowego stosowania środków organizacyjnych;
   f. informują Administratora o przetwarzaniu nowych zbiorów danych osobowych.
5. **Osoby upoważnione do przetwarzania danych** realizują zadania w zakresie ochrony danych osobowych zawartych w zbiorach, do których mają dostęp, a w szczególności zobowiązani są do:
   a. przestrzegania zasad przetwarzania danych osobowych zapisanych w dokumentacji bezpieczeństwa przetwarzania danych osobowych;

b. przekazywania IOD oraz bezpośredniemu przełożonemu wszelkich niezgodności związanych z ochroną danych osobowych;
c. informowania IOD o zmianach zaistniałych w przetwarzanych zbiorach;
d. niezwłocznego powiadomienia bezpośredniego przełożonego i IOD w sytuacji, gdy pracownik uzna, że dane osobowe zostały bądź są bezprawnie przetwarzane.

ROZDZIAŁ III

OBOWIĄZEK INFORMACYJNY I DOSTĘP DO DANYCH OSOBOWYCH

1. **Informacje podawane w przypadku pozyskiwania danych osobowych:**
   1) Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są bezpośrednio od tej osoby, Administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:
      a. swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
      b. gdy ma to zastosowanie – dane kontaktowe IOD;
      c. cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
      d. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią;
      e. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
      f. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
      g. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
      h. informacje o prawie do żądania od Administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
      i. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
      j. informacje o prawie wniesienia skargi do Organu Nadzorczego;
      k. informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
      l. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.
   2) Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, Administrator podaje osobie dodatkowo informacje o źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych.
   3) Wzór klauzuli informacyjnej w przypadku gdy dane zbierane są bezpośrednio od osoby stanowi załącznik Nr 1 do niniejszej Polityki. W przypadku zbierania danych z innych źródeł stosujemy wzór klauzuli stanowiący załącznik Nr 2 do niniejszej Polityki.

2. **Prawo dostępu przysługujące osobie, której dane dotyczą:**
   1) Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
      a. cele przetwarzania;
      b. kategorie danych osobowych;
      c. informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
      d. w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
      e. informacje o prawie do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
      f. informacje o prawie wniesienia skargi do Organu Nadzorczego;
      g. jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;
      h. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.
   2) Administrator prowadzi ewidencję realizacji praw wobec osób, których dane dotyczą, która stanowi załącznik Nr 3 do niniejszej Polityki.

ROZDZIAŁ IV

PRZETWARZANIE Z UPOWAŻNIENIA ORAZ W IMIENIU ADMINISTRATORA

1. **Administrator zezwala na przetwarzanie danych** osobowych w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych, nadawane przez Administratora lub osobę przez niego upoważnioną.
2. **Upoważnienie**, o którym mowa w niniejszym rozdziale, nadawane jest w formie pisemnej, indywidualnie, w zakresie zgodnym z zakresem obowiązków danego pracownika.
3. **Wzór upoważnienia** stanowi załącznik Nr 4 do niniejszej Polityki.
4. **Upoważnienia wydawane są zgodnie z następującą procedurą:**
   a. Osoba na stanowisku ds. pracowniczych przygotowuje upoważnienia do przetwarzania danych osobowych.
   b. Administrator lub osoba upoważniona przez Administratora podpisuje upoważnienie.
   c. Osoba na stanowisku ds. pracowniczych aktualizuje ewidencję osób upoważnionych do przetwarzania danych osobowych.
   d. Upoważnienia do przetwarzania danych osobowych przygotowywane są w ilości 2 egzemplarzy i przechowywane w teczce zawierającej wszystkie upoważnienia oraz w aktach osobowych danego pracownika.

5. **Ewidencja osób upoważnionych** do przetwarzania danych osobowych przechowywana jest w sposób uniemożliwiający dostęp osób nieupoważnionych. Wzór ewidencji stanowi załącznik Nr 5 do niniejszej Polityki.
6. **Powierzenie przetwarzania danych** osobowych innemu podmiotowi może nastąpić wyłącznie w drodze umowy zawartej w formie pisemnej przez administratora z podmiotem przetwarzającym z uwzględnieniem wymagań określonych w art. 28 rozporządzenia.
7. **Wzór umowy powierzenia** przetwarzania danych osobowych stanowi załącznik Nr 6 do niniejszej Polityki. Dopuszcza się zawierania umów w innej formie niż wskazana w załączniku nr 6, pod warunkiem, że umowa ta spełnia wymagania o których mowa w art. 28 rozporządzenia.
8. **Administrator prowadzi ewidencję umów powierzenia**, wzór ewidencji stanowi załącznik Nr 7 do niniejszej Polityki.

ROZDZIAŁ V

UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. **Zasady udostępniania danych:**
   1) Do udostępniania posiadanych w zbiorach danych osobowych upoważnieni są kierownicy działów, samodzielne stanowiska lub pracownik posiadający wymagane upoważnienie;
   2) Administrator udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa wyłącznie na pisemny umotywowany wniosek;
   3) Wszystkie udostępnienia są ewidencjonowane, wzór ewidencji stanowi załącznik Nr 8 do niniejszej Polityki. Ewidencja zawiera informacje o tym, komu udostępniono, datę kiedy zostały udostępnione oraz jaki zakres danych został udostępniony.
2. **Procedura przekazywania danych:**
   1) Podczas przekazywania dane zabezpiecza się przed ich nieuprawnionym dostępem;
   2) Dane przesyłane drogą teleinformatyczną muszą być odpowiednio zabezpieczone przed utratą ich poufności i integralności za pomocą zabezpieczeń kryptograficznych, umożliwiających ich bezpieczne przesyłanie.

ROZDZIAŁ VI

REJESTROWANIE CZYNNOŚCI PRZETWARZANIA DANYCH

1. **Rejestr czynności przetwarzania danych osobowych**
   1) Administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. W rejestrze tym zamieszcza wszystkie następujące informacje:
      a. swoją nazwę oraz dane kontaktowe oraz dane kontaktowe Inspektora Ochrony Danych;
      b. cele przetwarzania;

c. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
f. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 rozporządzenia.

2) Administrator podaje w rejestrze dodatkowo inne informacje, o których mowa we wzorze rejestru czynności przetwarzania danych, który stanowi załącznik Nr 9 do niniejszej Polityki.
3) Rejestr ma formę pisemną, w tym w formę elektroniczną.
4) Administrator udostępnia rejestr na żądanie Organu Nadzorczego.

2. **Rejestr kategorii czynności przetwarzania**

W jednostce prowadzi się rejestr wszystkich kategorii czynności dokonywanych w imieniu innych administratorów, zawierający następujące informacje:

a. imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
b. kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
c. gdy ma to zastosowanie – informację o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
d. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 rozporządzenia.

2) W rejestrze podaje się dodatkowo inne informacje, o których mowa we wzorze rejestru kategorii czynności przetwarzania danych, który stanowi załącznik Nr 10 do niniejszej Polityki.
3) Rejestr ma formę pisemną, w tym w formę elektroniczną.
4) Administrator udostępnia rejestr na żądanie Organu Nadzorczego.

ROZDZIAŁ VII

POSTĘPOWANIE W PRZYPADKU WYSTĄPIENIA NARUSZENIA OCHRONY DANYCH

1. **W przypadku naruszenia ochrony danych osobowych**, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Organowi Nadzorczemu właściwemu zgodnie z art. 55 rozporządzenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób

fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. **Zgłoszenie,** o którym mowa w pkt 1, musi co najmniej:
    a. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
    b. zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
    c. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
    d. opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym zastosowanych środków w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. **IOD lub osoba upoważniona dokumentuje wszelkie naruszenia** ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
4. **Sposób udokumentowania naruszeń** o którym mowa w pkt 3, opisuje Instrukcja postępowania w sytuacji naruszenia ochrony danych.
5. **Każdy pracownik Administratora** jest zobowiązany do niezwłocznego poinformowania bezpośredniego przełożonego, IOD oraz w przypadku danych osobowych przetwarzanych z użyciem systemu informatycznego służącego do przetwarzania danych osobowych - ASI, o każdym przypadku złamania zasad przetwarzania danych, a w szczególności o sytuacjach ujawnienia danych osobom nieuprawnionym.

ROZDZIAŁ VIII

ANALIZA RYZYKA BEZPIECZEŃSTWA INFORMACJI

1. **Proces zarządzania ryzykiem w bezpieczeństwie informacji składa się z:**
    1) ustanowienia kontekstu,
    2) szacowania ryzyka,
        a. analiza ryzyka
        b. ocena ryzyka
    3) postępowania z ryzykiem,
    4) akceptowania ryzyka,
    5) informowania o ryzyku oraz monitorowania i przeglądu ryzyka.
2. **Przebieg procesu:**
    1) W pierwszej fazie ustanawiany jest kontekst. Wybierane jest odpowiednie podejście odnosząc się do kryteriów oceny ryzyka, kryteriów skutków oraz kryteriów akceptowania ryzyka.
    2) Druga faza to przeprowadzanie szacowania ryzyka, w skład którego wchodzą analiza ryzyka oraz ocena ryzyka. Jeśli w wyniku szacowania ryzyka uzyska się informacje wystarczające do skutecznego określenia działań wymaganych w celu zmodyfikowania ryzyka do akceptowalnego poziomu, to następuje trzecia faza – postępowanie z ryzykiem. Jeżeli informacje są niewystarczające, to jest przeprowadzana następna iteracja szacowania

ryzyka przy zmienionym kontekście (kryteriów oceny ryzyka, kryteriów akceptacji ryzyka lub kryteriów skutków).

3) W ramach postępowania z ryzykiem określany jest akceptowalny poziom ryzyka, który poddany zostaje do akceptacji przez kierownictwo. Na jego podstawie przygotowany zostaje Plan postępowania z ryzykiem, który zostaje wdrożony w celu złagodzenia ryzyka bezpieczeństwa informacji.
4) Jest możliwe, że postępowanie z ryzykiem nie doprowadzi bezpośrednio do akceptowalnego ryzyk szczątkowych - czyli poziomu ryzyka po wdrożeniu zabezpieczeń. W takiej sytuacji jest potrzebna następna iteracja szacowania ryzyka ze zmienionymi parametrami kontekstu. Po tej iteracji następuje kolejne postępowanie z ryzykiem.
5) Działanie akceptowania ryzyka powinno zapewnić, że ryzyka szczątkowe są świadomie zaakceptowane przez kierownictwo organizacji.
6) Ostatnią fazy jest monitorowanie i utrzymywanie bezpieczeństwa poprzez przeglądy, planowane okresowe analizy ryzyka, nieplanowane analizy w wyniku informowania o ryzyku, reakcji na incydenty, zmian w systemie bezpieczeństwa.

ROZDZIAŁ IX

OCENA SKUTKÓW DLA OCHRONY 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. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.
2. **Ocena skutków dla ochrony danych, jest wymagana** w szczególności w przypadku:
   1) Systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
   2) Przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 rozporządzenia;
   3) W przypadku systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
3. **Ocena skutków zawiera co najmniej:**
   1) Systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
   2) Ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
   3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w pkt 1;
   4) Środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

ROZDZIAŁ X

OGÓLNE ZASADY BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

1. Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania.
2. Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
3. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem, w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
5. Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.
7. Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.
8. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. czystego biurka, która oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety.
9. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
10. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
11. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.
12. Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym.
13. Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).
14. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.

15. Na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.
16. Dane osobowe przesyłane elektronicznie powinny być zabezpieczone hasłem. Hasło to powinno być wysyłane oddzielnym kanałem telekomunikacyjnym.

ROZDZIAŁ XI

POSTANOWIENIA KOŃCOWE

1. **Wobec osoby, która w przypadku naruszenia** ochrony danych osobowych, zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także nie zrealizowała stosownego działania dokumentującego ten przypadek, może być podstawą do wszczęcia postępowania ws. ciężkiego naruszenia obowiązków pracowniczych.
2. **Inspektor Ochrony Danych zobowiązany jest** do przeprowadzania przeglądu polityki bezpieczeństwa przynajmniej raz w roku. Przegląd powinien się opierać przede wszystkim na zgodności polityki bezpieczeństwa z aktami prawa oraz wewnętrznymi dokumentami.
3. **Polityka bezpieczeństwa** jak i dokumenty będące załącznikami do polityki bezpieczeństwa obowiązują wszystkich pracowników Administratora.
4. **Procedury i zasady zawarte w niniejszym dokumencie** jak i jego załącznikach obowiązują, także stażystów, praktykantów oraz inne osoby, które mają dostęp do przetwarzania danych osobowych u Administratora.
5. **Postępowanie określone w ust. 1,** nie wyklucza odpowiedzialności karnej wobec tej osoby zgodnie z przepisami prawa oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
6. **W sprawach nieuregulowanych** niniejszym dokumentem mają zastosowanie przepisy rozporządzenia oraz ustawy o ochronie danych osobowych.

Otrzymują:
- wszystkie komórki organizacyjne Zakładu

DYREKTOR ZAKŁADU
inż. Ryszard Misiek

ZAŁĄCZNIK Nr 1

KLAUZULA INFORMACYJNA – WZÓR OGÓLNY (dane bezpośrednio od osoby)

1) Administratorem Pana/Pani danych osobowych jest ..... z siedzibą w ..... przy ul. ..... Może się Pan/Pani z nim skontaktować drogą elektroniczną na adres e-mail ....., telefonicznie pod numerem ..... lub tradycyjną pocztą na adres wskazany powyżej.
(dodatkowo należy podać dane przedstawiciela, jeżeli istnieje)*

2) W sprawach związanych z Pana/Pani danymi proszę kontaktować się z Inspektorem Ochrony Danych pod adresem e-mail .....

3) Pana/Pani dane osobowe będą przetwarzane w celu ..... na podstawie .....
(należy wskazać podstawę prawną przetwarzania, np. realizację umowy, zgodę; jeśli podstawą przetwarzania jest realizacja prawnie uzasadnionego interesu, należy wskazać, jaki to interes)*

4) W niektórych sytuacjach Pana/Pani dane osobowe mogą być udostępniane, jeśli będzie to konieczne do wykonywania ustawowych zadań. Będziemy przekazywać dane wyłącznie:
- podmiotom przetwarzającym, którym zlecimy przetwarzanie Pana/Pani danych,
- innym odbiorcom danych, np. bankom, ubezpieczycielom, kancelariom prawnym.

5) Pana/Pani dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.

6) Pana/Pani dane osobowe będą przechowywane przez okres .....
(jeżeli nie ma możliwości wskazania okresu przechowywania, należy podać kryterium ustalania tego okresu, np. do czasu zakończenia rekrutacji itd.)*

7) Ma Pan/Pani prawo dostępu do swoich danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania.

8) Ma Pan/Pani prawo wniesienia sprzeciwu wobec przetwarzania.

9) Ma Pan/Pani prawo do cofnięcia zgody w dowolnym momencie. Skorzystanie z prawa do cofnięcia zgody nie ma wpływu na przetwarzanie, które miało miejsce do momentu wycofania zgody.
(ma zastosowanie, jedynie gdy przetwarzanie odbywa się na podstawie zgody)*

10) Ma Pan/Pani także prawo do przenoszenia danych.
(ma zastosowanie, jedynie gdy przetwarzanie odbywa się na podstawie zgody wyrażonej przez osobę, której dane dotyczą, lub umowy, której jest stroną)*
11) Przysługuje Panu/Pani prawo wniesienia skargi do Organu Nadzorczego, gdy stwierdzi Pan/Pani naruszenie przetwarzania danych osobowych Pana/Pani dotyczących.

12) Podanie przez Pana/Panią danych osobowych jest ..... (wskazać, czy jest to wymóg ustawowy, warunek zawarcia umowy itd.).
Jest Pan/Pani zobowiązany/a do ich podania, a konsekwencją niepodania danych osobowych będzie ..... (wskazać konsekwencję niepodania danych, np. niemożliwość zawarcia umowy).

13) Pana/Pani dane będą/nie będą* przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania. Zautomatyzowane podejmowanie decyzji będzie odbywało się w celu ..... (wskazać cel profilowania, np. dopasowanie oferty do Pana/Pani potrzeb), a konsekwencją takiego przetwarzania może być ..... (wskazać konsekwencje profilowania, np. automatyczna odmowa zawarcia umowy na podstawie analizy wykonanej przez system).

ZAŁĄCZNIK Nr 2

KLAUZULA INFORMACYJNA – WZÓR OGÓLNY (dane z innych źródeł)

1) Administratorem Pana/Pani danych osobowych jest ..... z siedzibą w ..... przy ul. ..... Może się Pan/Pani z nim skontaktować drogą elektroniczną na adres e-mail ....., telefonicznie pod numerem ..... lub tradycyjną pocztą na adres wskazany powyżej.
(dodatkowo należy podać dane przedstawiciela, jeżeli istnieje)*

2) W sprawach związanych z Pana/Pani danymi proszę kontaktować się z Inspektorem Ochrony Danych pod adresem e-mail .....

3) Pana/Pani dane osobowe będą przetwarzane w celu ..... na podstawie .....
(należy wskazać podstawę prawną przetwarzania, np. realizację umowy, zgodę; jeśli podstawą przetwarzania jest realizacja prawnie uzasadnionego interesu, należy wskazać, jaki to interes)*

4) Administrator przetwarza następujące kategorie Pana/Pani danych osobowych ..... (wskazać kategorie przetwarzanych danych, np. imię i nazwisko, adres e-mail, adres zamieszkania, numer telefonu, PESEL itd.).

5) Administrator pozyskał Pana/Pani dane osobowe ze źródeł ..... (prywatnych/ publicznych) od ..... z siedzibą w ..... przy ul. .....

6) W niektórych sytuacjach Pana/Pani dane osobowe mogą być udostępniane, jeśli będzie to konieczne do wykonywania naszych usług. Będziemy przekazywać dane wyłącznie:
- podmiotom przetwarzającym, którym zlecimy przetwarzanie Pana/Pani danych,
- innym odbiorcom danych, np. bankom, ubezpieczycielom, kancelariom prawnym.

7) Pana/Pani dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.

8) Pana/Pani dane osobowe będą przechowywane przez okres .....
(jeżeli nie ma możliwości wskazania okresu przechowywania, należy podać kryterium ustalania tego okresu, np. do czasu wyłonienia zwycięscy konkursu, do czasu zakończenia rekrutacji itd.)*

9) Ma Pan/Pani prawo dostępu do swoich danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania.

10) Ma Pan/Pani prawo wniesienia sprzeciwu wobec przetwarzania.

11) Ma Pan/Pani prawo do cofnięcia zgody w dowolnym momencie. Skorzystanie z prawa do cofnięcia zgody nie ma wpływu na przetwarzanie, które miało miejsce do momentu wycofania zgody. *(* ma zastosowanie, jedynie gdy przetwarzanie odbywa się na podstawie zgody)*

12) Ma Pan/Pani także prawo do przenoszenia danych.
(ma zastosowanie, jedynie gdy przetwarzanie odbywa się na podstawie zgody wyrażonej przez osobę, której dane dotyczą, lub umowy, której jest stroną)*

13) Przysługuje Panu/Pani prawo wniesienia skargi do Organu Nadzorczego, gdy stwierdzi Pan/Pani naruszenie przetwarzania danych osobowych Pana/Pani dotyczących.

14) Pana/Pani dane będą/nie będą* przetwarzane w sposób zautomatyzowany w tym również w formie profilowania. Zautomatyzowane podejmowanie decyzji będzie odbywało się w celu ..... (wskazać cel profilowania, np. dopasowanie oferty do Pana/Pani potrzeb), a konsekwencją takiego przetwarzania może być ..... (wskazać konsekwencje profilowania, np. automatyczna odmowa zawarcia umowy na podstawie analizy wykonanej przez system).

ZAŁĄCZNIK Nr 3

EWIDENCJA REALIZACJI PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ				
Lp.	***Dane osoby***	***Rodzaj prawa***	***Podjęte działania***	***Uwagi***
1				
2				
3				
4				
5				

ZAŁĄCZNIK Nr 4

UPOWAŻNIENIE

Na podstawie art. 29 Rozporządzenia 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, zwane dalej „rozporządzeniem".

Upoważniam Panią/Pana

Zatrudnioną/Zatrudnionego na stanowisku

Do przetwarzania danych osobowych w formie papierowej oraz do obsługi systemu informatycznego służącego do przetwarzania danych osobowych u Administratora w zakresie zgodnym z wykonywaną pracą oraz otrzymanymi poleceniami służbowymi. Upoważnienie traci moc z chwilą ustania stosunku pracy/stażu/praktyki.

Zadania i czynności do wykonywania

1. Ochrona danych osobowych w systemie informatycznym i ręcznym, a w szczególności przeciwdziałanie dostępowi osób niepowołanych oraz przeciwdziałanie w przypadku wykrycia naruszeń zabezpieczeń systemu.
2. Przestrzeganie zasad określonych w Polityce bezpieczeństwa, Instrukcji określającej sposób zarządzania systemem informatycznym oraz w Instrukcji postępowania w sytuacji naruszania ochrony danych.

.....

Podpis Administratora lub osoby

upoważnionej do wystawiania upoważnień

Oświadczam, że zapoznałem(łam) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z rozporządzeniem oraz ustawą z dnia 10 maja 2018r. o ochronie danych osobowych i zobowiązuję się do ich przestrzegania.
Oświadczam ponadto, że zapoznałem(łam) się z wewnętrzną dokumentacją to jest: Polityką bezpieczeństwa przetwarzania danych osobowych oraz instrukcją określającą sposób zarządzania systemem informatycznym, służącym przetwarzaniu danych osobowych ze szczególnym uwzględnieniem bezpieczeństwa informacji i instrukcją postępowania w sytuacji naruszenia ochrony danych.
Świadomy(a) odpowiedzialności porządkowej i karnej oświadczam, że znane mi dane osobowe będę przetwarzać zgodnie z prawem, i nie dopuszczę do bezprawnego naruszenia tajemnicy również w sytuacji, gdy ustanie moje zatrudnienie u Administratora.

.....

Podpis osoby upoważnionej

Kliknij lub naciśnij tutaj, aby wprowadzić tekst.
Miejscowość

Kliknij lub naciśnij, aby wprowadzić datę.
Data

ZAŁĄCZNIK Nr 5

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH						
Lp.	*Nazwisko i Imię*	*Identyfikator (login do systemów)*	*Data nadania upoważnienia*	*Data odebrania upoważnienia*	*Zakres*	*Uwagi*
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
...						

ZAŁĄCZNIK Nr 6

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:

(zwana dalej „**Umową**")

_____

zwany w dalszej części „**Administratorem**"

reprezentowanym przez:

_____

a

_____

zwany w dalszej części „**Podmiotem przetwarzającym**"

(*dane podmiotu, który będzie przetwarzać dane osobowe w imieniu Administratora*)

reprezentowanym przez:

_____

zwane też w dalszej części „**Stronami**"

Niniejsza umowa została zawarta na podstawie przepisów dotyczących Rozporządzenia 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) zwane w dalszej części „**Rozporządzeniem**".

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu, w trybie art. 28 Rozporządzenia, dane osobowe do przetwarzania na zasadach i w celu określonym w niniejszej Umowie.
2. Administrator oświadcza, że jest Administratorem danych, które powierza Podmiotowi przetwarzającemu.
3. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

4. Podmiot przetwarzający oświadcza, że stosuje środki bezpieczeństwa spełniające wymogi RODO określone w § 3 ust. 1 niniejszej Umowy.

§ 2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie niniejszej Umowy następujące rodzaje danych osobowych oraz kategorie osób, których dane dotyczą:
   .....
   .....
   (rodzaje danych osobowych: zwykłe/szczególnej kategorii/dotyczące wyroków skazujących i naruszeń prawa,
   przykładowe kategorie osób, których dane dotyczą: pracownicy/klienci/kontrahenci Administratora w postaci np. imion i nazwisk/adresów zamieszkania/PESEL)
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu .....
   (np. w celu realizacji umowy z dnia ..... w zakresie świadczenia usług kadrowo-płacowych)

§ 3

Obowiązki i prawa Stron

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających odpowiedni stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia m. in.:
   a) pseudonimizacja i szyfrowanie danych osobowych;
   b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
   c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
   d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
2. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej Umowy.
3. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust. 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
4. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/zwraca (*należy wybrać*) Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
5. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
6. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych niezwłocznie zgłasza je Administratorowi jednak nie później niż w ciągu 48 godzin.

7. Administrator zgodnie z art. 28 ust. 3 pkt h Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy.
8. Administrator realizować będzie prawo kontroli wyłącznie w godzinach pracy Podmiotu przetwarzającego i nie wcześniej niż po upływie ... *(np. 7)* dni od dnia zawiadomienia.
9. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora, jednak nie dłuższym niż ... *(np. 7)* dni. W przypadku, gdyby usunięcie uchybień wiązałoby się z poniesieniem dużego nakładu finansowego lub organizacyjnego, termin ten może zostać przedłużony do 30 dni.
10. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§ 4

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą Umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania Umowy po uzyskaniu uprzedniej pisemnej zgody Administratora.
2. Podmiot przetwarzający zobowiązuje się do korzystania z usług wyłącznie takich podwykonawców, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie przez tych podwykonawców danych osobowych, spełniało wymogi Rozporządzenia.
3. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
4. Podwykonawca winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
5. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 5

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie, a także:

   1) o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego,

   2) o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez organ nadzorczy. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora.

§ 6

Czas obowiązywania Umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas ..... *(nieokreślony/określony od ..... do .....)*
2. Każda ze stron może wypowiedzieć niniejszą Umowę z zachowaniem ..... (*np. miesięcznego*) okresu wypowiedzenia.

§ 7

Rozwiązanie umowy

1. Administrator może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z Umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora.

§ 8

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne"). Podjęte zobowiązanie pozostaje w mocy w czasie trwania i po zakończeniu przetwarzania w ramach powierzenia danych osobowych.
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora w innym celu niż wykonania Umowy, chyba że konieczność ujawnienia informacji wynika z obowiązujących przepisów prawa lub Umowy.

§ 9

Postanowienia końcowe

1. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
2. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze Stron.
3. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
4. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy Administratora/Podmiotu przetwarzającego (*należy wybrać*).

_____ _____

Administrator Podmiot przetwarzający

ZAŁĄCZNIK Nr7

EWIDENCJA UMÓW POWIERZENIA				
Lp.	*Nr umowy*	*Okres obowiązywania*	*Nazwa podmiotu przetwarzającego*	*Powierzone czynności przetwarzania*
1				
2				
...				

ZAŁĄCZNIK Nr 8

EWIDENCJA UDOSTĘPNIEŃ DANYCH OSOBOWYCH					
Lp.	***Odbiorca danych***	***Data udostępnienia***	***Udostępniający***	***Zakres danych udostępnionych***	***Uwagi***
1					
2					
...					

ZAŁĄCZNIK Nr 9

REJESTR CZYNNOŚCI PRZETWARZANIA	
Nazwa i dane kontaktowe administratora	
Nazwa	
Adres	
E-mail	
Telefon	
Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	
Adres	
E-mail	
Telefon	
Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
E-mail	
Telefon	

Nazwa czynności przetwarzania		
Jednostka organizacyjna (departament, dział itp.)		
Cel przetwarzania Art. 30 ust. 1 pkt b		
Kategorie osób Art. 30 ust. 1 pkt c		
Kategorie danych osobowych Art. 30 ust. 1 pkt c		
Podstawa prawna		
Źródło danych		
Planowany termin usunięcia kategorii danych (jeżeli jest to możliwe) Art. 30 ust. 1 pkt f		
Nazwa współadministratora i dane kontaktowe (jeśli dotyczy) Art. 30 ust. 1 pkt d		
Nazwa podmiotu przetwarzającego i dane kontaktowe (jeśli dotyczy) Art. 30 ust. 1 pkt d		
Kategorie odbiorców (innych niż podmiot przetwarzający) Art. 30 ust. 1 pkt d		
Nazwa systemu lub oprogramowania		
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 (jeżeli jest to możliwe) Art. 30 ust. 1 pkt g		
DPIA (jeśli tak, lokalizacja raportu)		
Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu) Art. 30 ust. 1 pkt e		
Jeśli transfer i art. 49 ust. 1 akapit drugi – dokumentacja odpowiednich zabezpieczeń Art. 30 ust. 1 pkt e		

ZAŁĄCZNIK Nr 10

REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA	
Nazwa i dane kontaktowe podmiotu przetwarzającego	
Nazwa	
Adres	
E-mail	
Telefon	
Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	
Adres	
E-mail	
Telefon	
Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
E-mail	
Telefon	

Kategorie przetwarzań		(nazwa kategorii czynności)	.....	.....	.....
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)					
Administrator	Nazwa i dane kontaktowe administratora				
	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)				
	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)				
	Inspektor ochrony danych administratora (jeśli powołano)				
Czas trwania przetwarzania					
Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane					
Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi					
Podprzetwarzający (podwykonawca) - jeśli dotyczy	Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)				
	Kategorie podpowierzonych przetwarzań				