ZARZĄDZENIE NR 2/2022
DYREKTORA ZAKŁADU AKTYWNOŚCI ZAWODOWEJ
w BYDGOSZCZY
z dnia 13.06.2022 roku

w sprawie wprowadzenia Polityki ochrony danych osobowych
Zakładu Aktywności Zawodowej w Bydgoszczy

§ 1

Na podstawie § 9 ust. 1 Statutu Zakładu Aktywności Zawodowej stanowiącego załącznik do uchwały Nr LXXVII/1154/10 Rady Miasta Bydgoszczy z dnia 27 października 2010 roku w sprawie zmiany uchwały Nr LIV/1086/05 Rady Miasta Bydgoszczy w sprawie utworzenia jednostki organizacyjnej miasta – Zakładu Aktywności Zawodowej w Bydgoszczy, 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 (Dz. Urz. UE. L 119/1), ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. z 2019 r., poz. 1781), Dyrektor Zakładu Aktywności Zawodowej w Bydgoszczy zarządza, co następuje.

§ 2

Wprowadza się Politykę ochrony danych osobowych Zakładu Aktywności Zawodowej w Bydgoszczy, stanowiącą załącznik nr 1 do niniejszego zarządzenia

§ 3

1. Administratorem danych osobowych pracowników, praktykantów oraz osób zatrudnionych na podstawie umów cywilnoprawnych jest Zakład Aktywności Zawodowej w Bydgoszczy (zwany dalej Zakładem).
2. Osobą reprezentującą Zakład we wszystkich sprawach związanych z ochroną danych osobowych jest Dyrektor.

§ 4

1. Zobowiązuje się wszystkich pracowników Zakładu do zapoznania się z treścią dokumentu wymienionego w § 1 i bezwzględnego stosowania się do zawartych w nim regulacji.
2. Zobowiązuje się wszystkich pracowników Zakładu do podpisania oświadczenia o zapoznaniu się Polityką ochrony danych osobowych i dostarczenia go do samodzielnej komórki ds. adm. – gosp. w terminie do dnia 20 czerwca 2022 roku.
3. Wzór oświadczenia, o którym mowa w ust. 2 stanowi Załącznik nr 3 do Polityki ochrony danych osobowych.

4. Pracownicy nieobecni w pracy w dniu wejścia w życie niniejszego zarządzenia, zobowiązani są do podpisania oświadczenia, o którym mowa w ust. 2, w pierwszym tygodniu po powrocie do pracy.
5. Nadzór nad wykonaniem obowiązków opisanych w ust. 1-4 powierza się do realizacji samodzielnej komórce ds. adm. – gosp.
6. Oświadczenie, o którym mowa w ust. 2 przechowuje się w teczce akt personalnych pracownika, zaś wykaz osób które złożyły oświadczenia, należy przekazać niezwłocznie do Inspektora Ochrony Danych.

§ 5

Traci moc zarządzenie Dyrektora Zakładu Aktywności Zawodowej w Bydgoszczy nr 4/2019 z dnia 3 lipca 2019 r.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Zakładu Aktywności Zawodowej
w Bydgoszczy
Krzysztof Ciężki

Załącznik nr 1 do
Zarządzenia nr 2/2022 r. Dyrektora ZAZ
z dnia 13.06.2022 r.

Polityka Ochrony Danych Osobowych w Zakładzie Aktywności Zawodowej w Bydgoszczy

Rozdział 1
Postanowienia ogólne

§ 1

Polityka ochrony danych osobowych w Zakładzie Aktywności Zawodowej w Bydgoszczy, zwana dalej „Polityką", została opracowana na podstawie art. 24 ust. 2 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), zwanego dalej „Rozporządzeniem".

§ 2

Ilekroć w Polityce jest mowa o:

a) **Administratorze Danych** – rozumie się przez to Zakład Aktywności Zawodowej w Bydgoszczy (zwanej dalej Administratorem Danych albo Zakładem);
b) **Aplikacji** – rozumie się przez to program użytkowy, konkretny – ze względu na oferowaną użytkownikom funkcjonalność, element oprogramowania użytkowego;
c) **Autoryzacji** – rozumie się przez to proces przyznawania użytkownikowi określonych uprawnień dostępu lub korzystania z zasobów danego programu, aplikacji lub systemu;
d) **Danych osobowych** – rozumie się przez to 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;
e) **Elektronicznym nośniku informacji** – rozumie się przez to narzędzie lub urządzenie służące do zbiorowego składowania oraz odczytu zebranych informacji, w tym w szczególności: dyskietkę, płytę CD lub DVD, dysk twardy, pen drive, flash disc, aparat fotograficzny, taśmę streamera, dysk magnetooptyczny oraz taśmę magnetyczną;
f) **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
g) **Identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę uprawnioną do przetwarzania danych osobowych w systemie informatycznym;
h) **Integralności danych** – rozumie się przez to właściwość polegającą na zapewnieniu dokładności i kompletności danych osobowych;
i) **Samodzielnym stanowisku** – osoba realizująca samodzielnie zadania Zakładu wskazane przez Dyrektora Zakładu w umowie o pracę, bądź zakresie czynności;
j) **IOD lub Inspektor** – oznacza Inspektora Ochrony Danych Osobowych;
k) **Naruszeniu ochrony danych osobowych** – rozumie się przez to 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;
l) **Odbiorcy** – rozumie się przez to 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 dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej 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;
m) **Organie nadzorczym** – rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych;
n) **Podmiocie przetwarzającym** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
o) **Poufności danych** – rozumie się przez to właściwość polegającą na tym, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;
p) **Przetwarzaniu** – rozumie się przez to 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;
q) **Rozliczalności** – rozumie się przez to rozliczalność, o której mowa w art. 5 ust. 2 Rozporządzenia;

r) **Utrwalaniu danych** – rozumie się przez to zapisywanie danych w sposób trwały na wszelkiego rodzaju nośnikach papierowych lub elektronicznych;
s) **Użytkowniku** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych w Zakładzie i uprawnioną do ich przetwarzania w systemach informatycznych;
t) **Zasobie teleinformatycznym** – rozumie się przez to system, program, aplikację lub udział sieciowy, w szczególności folder na dysku sieciowym, w którym przetwarzane są dane osobowe;
u) **Zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Rozdział 2
Cele i zakres Polityki

§ 1

Polityka określa podstawowe zasady ochrony danych osobowych.

§ 2

Polityka ma zastosowanie wobec:
a) osób upoważnionych do przetwarzania danych osobowych w Zakładzie;
b) wszystkich danych osobowych, przetwarzanych w Zakładzie, niezależnie od formy (tradycyjne, papierowe zbiory ewidencyjne, w systemach informatycznych) oraz miejsca przetwarzania;
c) wszystkich zasobów teleinformatycznych Zakładu, w których przetwarzane są dane osobowe.

§ 3

Celem Polityki jest opis realizacji w Zakładzie obowiązków wynikających z Rozporządzenia oraz zasad ochrony danych osobowych przetwarzanych w Zakładzie.

§ 4

Cele Polityki realizowane są poprzez zapewnienie zgodności przetwarzania danych osobowych z prawem, rzetelności, przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, a także poprzez bezpieczeństwo danych w tym zapewnienie integralności i poufności.

Rozdział 3
Obowiązki i odpowiedzialność w zakresie zarządzania ochroną danych osobowych

§ 1

Zakład jako Administrator Danych wykonuje obowiązki z zakresu przetwarzania i ochrony danych osobowych zgodnie z przepisami Rozporządzenia.

§ 2

Zakład stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpiecza dane osobowe przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

§ 3

Zadania, o których mowa w § 2 niniejszego rozdziału, w imieniu Zakładu, poza Inspektorem Ochrony Danych, wykonują osoby sprawujące samodzielne stanowiska w Zakładzie, w odniesieniu do danych osobowych przez te osoby przetwarzanych.

§ 4

Wszystkie osoby upoważnione do przetwarzania danych zobowiązane są do:
a) przetwarzania i ochrony danych osobowych zgodnie z obowiązującymi przepisami;

b) postępowania zgodnie z ustaloną przez Zakład Polityką;
c) ścisłego przestrzegania zakresu udzielonego upoważnienia;
d) zachowania w tajemnicy danych osobowych.

§ 5

Zakład wyznaczy Inspektora Ochrony Danych w Zakładzie.

§ 6

Do zadań Inspektora Ochrony Danych należy w szczególności:
a) monitorowanie przestrzegania Rozporządzenia oraz Polityki Ochrony Danych Osobowych Zakładu, realizacja działań zwiększających świadomość personelu uczestniczącego w operacjach przetwarzania;
b) podjęcie działań zgodnie z rozdziałem 8, w przypadku stwierdzenia naruszeń ochrony danych osobowych;
c) opiniowanie projektów umów o powierzenie przetwarzania danych osobowych;
d) monitorowanie sposobu przetwarzania danych osobowych przez osoby pełniące samodzielne stanowiska w Zakładzie;
e) informowanie Administratora Danych, oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia i doradzanie im w tej sprawie.

§ 7

Do zadań Inspektora Ochrony Danych ponadto należy:
a) prowadzenie rejestru czynności przetwarzania danych osobowych, o którym mowa w art. 30 Rozporządzenia;
b) prowadzenie ewidencji osób upoważnionych do przetwarzania danych;
c) współpraca z organem nadzorczym;
d) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem.

§ 8

1. Administrator Danych zapewni Politykę Bezpieczeństwa Informatycznego.
2. Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Zakładzie określa Załącznik nr 1 do niniejszej Polityki.

§ 9

W zakresie zapewnienia bezpieczeństwa przetwarzania danych osobowych w eksploatowanych systemach informatycznych i sieciach teleinformatycznych do zadań Administratora Danych należy:
a) dostosowanie systemów lub aplikacji oraz oprogramowania do wymogów, o których mowa w Rozporządzeniu;
b) nadzorowanie technicznego zabezpieczenia i odpowiedniego wyposażenia obszarów przetwarzania danych osobowych.

§ 10

1. Administrator Danych realizuje czynności w zakresie ochrony danych osobowych poprzez zapewnienie bezpieczeństwa fizycznego pomieszczeń i obiektów, które tworzą obszary przetwarzania danych.
2. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe stanowi Załącznik nr 2 do niniejszej Polityki.

§ 11

1. Do zadań Administratora Danych w zakresie ochrony danych osobowych, należy w szczególności wyposażenie obiektów i pomieszczeń, w których przetwarzane są dane osobowe właściwe środki ochrony i zapewnienie ich właściwego funkcjonowania.
2. Administrator Danych odpowiedzialny jest za zastosowanie w Zakładzie, technicznych i organizacyjnych środków zapewniających ochronę przetwarzanych danych osobowych.

§ 12

Osoby pełniące samodzielne stanowiska w Zakładzie są odpowiedzialne za przestrzeganie przepisów dotyczących przetwarzania i ochrony danych osobowych w zakresie wykonywanych przez te osoby zadań.

§ 13

Do zadań osób zajmujących samodzielne stanowiska w Zakładzie należy, w szczególności:

a) zapewnienie zachowania szczególnej staranności przy przetwarzaniu danych osobowych, z uwzględnieniem zasad zgodności z prawem, rzetelności, przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania;
b) wnioskowanie o rejestrację, aktualizację i usunięcie czynności z rejestru czynności prowadzonego przez Inspektora Ochrony Danych;
c) wypełnianie obowiązków informacyjnych, o których mowa w art. 13 i 14 Rozporządzenia;
d) rozpatrywanie, w porozumieniu z Inspektorem Ochrony Danych, skarg, wniosków i żądań osób, których dane dotyczą w związku z przetwarzaniem ich danych osobowych;
e) nadzór (w zakresie wykonywanych zadań) nad przestrzeganiem przepisów o ochronie danych osobowych.

Rozdział 4
Dopuszczalność przetwarzania danych osobowych

Przetwarzanie danych osobowych jest dopuszczalne po spełnieniu co najmniej jednej z przesłanek wymienionych w art. 6, 9 lub 10 Rozporządzenia i z uwzględnieniem zasad, o których mowa w art. 5 Rozporządzenia.

Rozdział 5
Obowiązki Informacyjne

§ 1

W przypadku zbierania danych osobowych od osoby, której one dotyczą, konieczne jest podanie tej osobie informacji zgodnie z art. 13 ust. 1-3 Rozporządzenia z zastrzeżeniem ust. 4 powołanego artykułu.

§ 2

W przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której one dotyczą, konieczne jest podanie tej osobie informacji zgodnie z art. 14 ust. 1-4 Rozporządzenia z zastrzeżeniem ust. 5 powołanego artykułu.

Rozdział 6
Zasady dopuszczania osób do przetwarzania danych osobowych

§ 1

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie od Administratora Danych, zapoznane z przepisami o ochronie danych osobowych oraz zobowiązane do zachowania danych osobowych w tajemnicy.
2. Administrator Danych kieruje pracownika, wolontariusza, osobę będącą stroną umowy cywilnoprawnej, praktykanta lub stażystę odpowiednio do Inspektora Ochron Danych w celu zapoznania z przepisami o ochronie danych osobowych i Polityką Ochrony Danych Osobowych obowiązującą w Zakładzie.
3. Inspektor Ochrony Danych odbiera pisemne oświadczenie o zapoznaniu z przepisami o ochronie danych osobowych i Polityką Ochrony Danych Osobowych obowiązującą w Zakładzie.
4. Wzór oświadczenia osoby przetwarzającej dane osobowe, stanowi Załącznik nr 3 do Polityki.
5. Upoważnienie do przetwarzania danych osobowych dla:
   a) pracowników zajmujących stanowisko, z którym wiąże się przetwarzanie danych osobowych jest opracowywane, przedkładane do podpisu oraz wydawane pracownikowi, podczas podpisywania umowy o pracę;
   b) stażystów, praktykantów lub wolontariuszy realizujących zadania, z którymi wiąże się przetwarzanie danych osobowych jest opracowywane, przedkładane do podpisu oraz wydawane, w dniu rozpoczęcia stażu, praktyk lub wolontariatu;
   c) osób wykonujących zadania na podstawie umów cywilnoprawnych – stanowi załącznik do umowy zawieranej z daną osobą.
6. Upoważnienie do przetwarzania danych osobowych nadawane jest na czas:
   a) trwania stosunku pracy;
   b) współpracy z osobą niebędącą pracownikiem.
7. Wzór upoważnienia do przetwarzania danych osobowych stanowi Załącznik nr 4 do niniejszej Polityki.

Rozdział 7
Przekazywanie, udostępnianie i powierzanie przetwarzania danych osobowych

§ 1

1. Przekazywanie danych wewnątrz Zakładu może następować wyłącznie pomiędzy osobami posiadającymi ważne upoważnienie do przetwarzania danych osobowych.
2. Zakres przekazywanych danych nie może wykraczać poza dane, których przetwarzanie jest niezbędne w ramach wykonywanych zadań przez osobę odbierającą dane osobowe.

§ 2

Dane osobowe przetwarzane w Zakładzie mogą być udostępnione na zewnątrz Zakładu jedynie na podstawie przepisów prawa.

§ 3

Dane osobowe mogą być udostępniane na wniosek osoby, której dane dotyczą, w ramach przysługującego jej prawa dostępu, zgodnie z art. 15 Rozporządzenia.

§ 4

W przypadku dokonywania zlecenia świadczenia usług, z którym wiąże się przetwarzanie, przez podmiot przetwarzający, danych osobowych w imieniu Zakładu, należy dokonać powierzenia przetwarzania danych osobowych stosownie do wymogów określonych w art. 28 Rozporządzenia.

§ 5

Powierzenie przetwarzania nastąpić może wyłącznie w drodze umowy zawartej na piśmie wiążącej Podmiot przetwarzający i Administratora Danych. Administratora Danych mogą reprezentować osoby przez niego upoważnione.

§ 6

Projekt umowy (porozumienia) o powierzenie przetwarzania danych osobowych wymaga uzgodnienia z Inspektorem Ochrony Danych.

§ 7

1. Rejestr powierzeń przetwarzania danych osobowych zawiera dane podmiotu przetwarzającego, przedmiot umowy, numer i datę zawarcia umowy.
2. Rejestr powierzeń jest prowadzony przez Inspektora Danych Osobowych w Zakładzie. Wzór rejestru powierzeń, stanowi Załącznik nr 10 do Polityki.
3. Wzór umowy o powierzenie przetwarzania danych osobowych, stanowi Załącznik nr 5 do Polityki.

Rozdział 8
Procedura postępowania w przypadku naruszenia ochrony danych osobowych

§ 1

Naruszenie ochrony danych osobowych następuje w szczególności w przypadku pożaru, w wyniku którego utracone zostaną dokumenty zawierające dane osobowe, zgubienia nośnika pendrive, laptopa, w których zapisane były pliki zawierające dane osobowe, ataku hakerskiego, którego skutkiem jest nieuprawniony dostęp do systemów teleinformatycznych, w których przetwarzane są dane osobowe.

§ 2

W przypadku stwierdzenia naruszenia ochrony danych osobowych, każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do:

a) niezwłocznego zawiadomienia o powyższym Inspektora Ochrony Danych. Jeżeli naruszenie lub okoliczności wskazujące na możliwość jego zaistnienia dotyczą danych osobowych przetwarzanych w systemach informatycznych należy ponadto zawiadomić o nich Administratora Danych;
b) powstrzymania się od wszelkich działań mogących spowodować zatarcie śladów, bądź dowodów naruszenia.

§ 3

Osoba pełniąca samodzielne stanowiska w Zakładzie zawiadamia o naruszeniu Inspektora Ochrony Danych, w miarę możliwości, nie później niż w terminie 24 godzin po stwierdzeniu naruszenia.

§ 4

Zawiadomienie, o którym mowa w § 3 powinno, co najmniej:
a) opisywać charakter naruszenia ochrony danych osobowych, w tym 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 osoby, od której można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

§ 5

Osoby pełniące samodzielne stanowiska w Zakładzie są obowiązane gromadzić wszelkie dokumenty związane z naruszeniem, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze i przekazywać je do Inspektora Ochrony Danych.

§ 6

Inspektor Ochrony Danych sporządza raport z naruszenia. Wzór raportu naruszenia ochrony danych osobowych, stanowi Załącznik nr 6 do Polityki.

§ 7

Inspektor ochrony Danych reaguje na naruszenia dotyczące danych osobowych przetwarzanych w systemach informatycznych, aby zmniejszyć ich skutki, a także aby zapobiec podobnym przypadkom w przyszłości.

§ 8

1. Osoby pełniące samodzielne stanowiska w Zakładzie są obowiązane do przekazywania Inspektorowi Ochrony Danych zgłoszeń naruszeń dokonywanych przez podmioty przetwarzające, w wykonaniu umów o powierzenie przetwarzania danych osobowych, których realizację nadzorują.
2. Inspektor Ochrony Danych na podstawie otrzymanych informacji i dokumentów przygotowuje Administratorowi Danych zgłoszenie naruszenia organowi nadzorczemu, a jeżeli jest wymagane, także zawiadomienie osoby, której dane dotyczą.

Rozdział 9
Archiwizacja i usuwanie danych osobowych

§ 1

Dane osobowe podlegają archiwizacji zgodnie z powszechnie obowiązującymi przepisami prawa.

§ 2

Usunięcie danych następuje gdy cel, dla którego zebrano dane został osiągnięty lub dane są już zbędne dla osiągnięcia tego celu.

§ 3

Zasada ograniczenia okresu przechowywania danych osobowych do ścisłego minimum ma zastosowanie do wszelkich form przetwarzania danych (papierowej i elektronicznej).

Rozdział 10
Rejestrowanie czynności przetwarzania danych osobowych

§ 1

Rejestr czynności przetwarzania danych osobowych jest prowadzony przez Inspektora Ochrony Danych.

§ 2

1. Rejestr czynności przetwarzania danych osobowych obejmuje w szczególności niżej wymienione informacje:
   a) cel przetwarzania;
   b) opis kategorii osób i kategorii danych jakie będą przetwarzane;
   c) podstawę prawną przetwarzania danych;
   d) odbiorców lub kategorię odbiorców, którym dane mogą być przekazywane;
   e) planowane terminy usunięcia poszczególnych kategorii danych;
   f) formę danych (papierowa, elektroniczna);
   g) ewentualne przekazywanie danych do państwa trzeciego lub organizacji międzynarodowych;
   h) opis fizycznych, technicznych i organizacyjnych środków bezpieczeństwa.
2. Wzór Rejestru czynności przetwarzania danych osobowych stanowi Załącznik nr 7 do Polityki.

Rozdział 11
Sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

§ 1

Monitorowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz Polityką w Zakładzie jest zadaniem Inspektor Ochrony Danych.

§ 2

Monitorowanie, o którym mowa w § 1 odbywa się w formie sprawdzeń.

§ 3

Sprawdzenia mogą być przeprowadzane w trybie sprawdzenia planowego lub doraźnego.

§ 4

Inspektor Ochrony Danych opracowuje plan sprawdzeń na dany rok i przedkłada go do wiadomości Administratorowi Danych.

§ 5

Inspektor Ochrony Danych ma prawo do:
a) wstępu do pomieszczeń, w których są przetwarzane dane osobowe;
b) żądania złożenia pisemnych lub ustnych wyjaśnień oraz okazania dokumentów i zrobienia ich kopii, przez osoby zatrudnione przy przetwarzaniu danych osobowych, w zakresie niezbędnym do przeprowadzenia sprawdzenia;
c) przeprowadzania oględzin urządzeń, nośników informacji i systemów informatycznych służących do przetwarzania danych osobowych.

§ 6

Inspektor Ochrony Danych sporządza sprawozdanie ze sprawdzenia, zawierające w szczególności przedmiot sprawdzenia, stwierdzone nieprawidłowości i propozycje działań mających na celu przywrócenie przetwarzania danych osobowych zgodnego z prawem.

§ 7

Inspektor Ochrony Danych przedkłada sprawozdanie Administratorowi Danych z dokonanych czynności sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w Zakładzie.

§ 8

W przypadku stwierdzenia nieprawidłowości, Administrator Danych decyduje o podjęciu działań naprawczych.

Rozdział 13
Środki ochrony

§ 1

Stosowane środki powinny uwzględniać stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

§ 2

Ochrona danych osobowych w Zakładzie zapewniana jest poprzez zastosowanie:
a) środków ochrony fizycznej ;
b) środków ochrony teleinformatycznej;
c) środków organizacyjnych.

§ 3

1. Zakład w celu ochrony danych osobowych gwarantuje właściwe zabezpieczenia pomieszczeń przed wejściem osób nieupoważnionych.
2. Zakład przechowuje dane osobowe w szafach zamykanych na klucz.

§ 4

Środki ochrony teleinformatycznej danych osobowych określa Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

§ 5

Do środków organizacyjnych zalicza się:
a) wyznaczenie Inspektora Ochrony Danych;
b) monitorowanie przestrzegania przepisów o ochronie danych osobowych;
c) dopuszczanie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie;
d) zapewnianie zapoznania osób przetwarzających dane osobowe z przepisami o ochronie danych osobowych;
e) zobowiązanie osób przetwarzających dane osobowe do zachowania danych osobowych w tajemnicy;
f) niszczenie dokumentów zawierających dane osobowe po ustaniu ich przydatności, za pomocą mechanicznych niszczarek dokumentów;
g) zakaz pozostawiania bez nadzoru dokumentów zawierających dane osobowe.

§ 6

W sprawach nieuregulowanych zastosowanie mają przepisy Rozporządzenia.

Rozdział 14
Załączniki do Polityki Ochrony Danych Osobowych

1. Załącznik nr 1 – „Instrukcja Zarządzania Systemem Informatycznym służąca do przetwarzania danych osobowych w Zakładzie";

2. Załącznik nr 2 – „Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w których przetwarzane są dane osobowe";
3. Załącznik nr 3 – „Wzór oświadczenia osoby przetwarzającej dane";
4. Załącznik nr 4 – „Wzór upoważnienia do przetwarzania danych osobowych";
5. Załącznik nr 5 – „Wzór umowy o powierzeniu przetwarzania danych";
6. Załącznik nr 6 – „Wzór Raportu naruszenia danych osobowych";
7. Załącznik nr 7 – „Wzór Rejestru czynności przetwarzania danych";
8. Załącznik nr 8 – „Ewidencja osób upoważnionych do przetwarzania danych osobowych".
9. Załącznik nr 9 – „Wykaz zbiorów danych i systemów zastosowanych do ich przetwarzania"

Załącznik nr 1
do Polityki Ochrony Danych Osobowych

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM służącym do przetwarzania danych osobowych w Zakładzie Aktywności Zawodowej w Bydgoszczy

1. CEL OPRACOWANIA DOKUMENTU

Celem niniejszego dokumentu jest określenie sposobu zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, używanymi w związku z prowadzeniem działalności przez Zakład Aktywności Zawodowej w Bydgoszczy (dalej jako „**Zakład**").

2. ZAKRES ZASTOSOWANIA

Instrukcja określa zasady zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych, a w szczególności:

a) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w Systemie Informatycznym;
b) metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
c) procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników Systemu;
d) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
e) sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych;
f) sposób zabezpieczenia Systemu Informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awariami zasilania;
g) sposoby realizacji w Systemie wymogów dotyczących przetwarzania danych;
h) procedury wykonywania przeglądów i konserwacji Systemu oraz nośników informacji służących do przetwarzania danych.

3. REJESTROWANIE I WYREJESTROWANIE UŻYTKOWNIKA – NADAWANIE UPRAWNIEŃ

1. Użytkownikiem Systemu Informatycznego, mającym dostęp do danych osobowych (osobą upoważnioną) może być osoba, której nadano upoważnienie do przetwarzania danych osobowych zgodnie ze wzorem stanowiącym Załącznik nr 4 do Polityki Ochrony Danych Osobowych,
2. Uzyskanie uprawnień następuje na dwóch poziomach:
    1) Zarejestrowanie w systemie (założenie konta),
    2) Nadanie upoważnienia do przetwarzania danych osobowych.
3. Osoba odpowiedzialna za obsługę informatyczną tworzy oraz modyfikuje konta dostępowe/pocztowe pracownika oraz ustawia dostęp do wybranych baz danych i aplikacji na podstawie informacji o nowym pracowniku oraz o wszelkich zmianach stanu zatrudnienia uzyskanych od administratora danych.
4. W przypadku zakończenia pracy w Zakładzie lub wygaśnięcia upoważnienia, o którym mowa w pkt. 3 ust. 2.2, osoba odpowiedzialna za obsługę informatyczną likwiduje konto po uzyskaniu informacji od bezpośredniego przełożonego pracownika lub innej upoważnionej osoby informację o zakończeniu pracy w Zakładzie. Wyrejestrowanie użytkownika (skasowanie konta dostępowego) jest jednoznaczne z uniemożliwieniem mu dostępu do systemu informatycznego (zablokowanie dostępu).
5. Uprawnienia osób upoważnionych do przetwarzania danych osobowych są rejestrowane w systemie informatycznym oraz odnotowywane w „Ewidencji osób upoważnionych do przetwarzania danych osobowych" stanowiącej Załącznik nr 8 do Polityki Ochrony Danych Osobowych. Wszystkie formularze i inne dokumenty związane z rejestrowaniem i wyrejestrowaniem użytkowników są archiwizowane i przechowywane.

4. SPOSÓB UWIERZYTELNIANIA UŻYTKOWNIKA I ZASADY KORZYSTANIA Z HASEŁ

1. Każdorazowe uwierzytelnienie użytkownika w systemie informatycznym następuje po podaniu identyfikatora i hasła.
2. W Zakładzie obowiązują następujące zasady korzystania z haseł:
    1) Hasło użytkownika:

a) Składa się z co najmniej 8 znaków,
b) Hasło musi zawierać co najmniej jedną małą literę, jedną wielką literę, jedną cyfrę oraz znaki specjalne,
c) Hasło do kont o uprawnieniach administratora są kilkunastoznakowe i zawierają co najmniej jedną małą literę, jedną wielką literę, jedną cyfrę oraz jeden znak specjalny,
d) Co 30 dni hasło musi zostać zmienione.

2) Elementy systemu informatycznego związane z bezpieczeństwem dostępu są tak sparametryzowane, aby wymusić stosowanie podanych zasad.
3) Niezastosowanie przez użytkownika zasad wskazanych pod lit. a), b) lub c) powoduje odmowę dostępu do systemu informatycznego.

3. Prawidłowe wykonywanie obowiązków związanych z korzystaniem przez użytkowników z haseł nadzoruje osoba odpowiedzialna za obsługę informatyczną. Nadzór ten w szczególności polega na okresowym monitorowaniu funkcjonowania mechanizmu uwierzytelniania.

5. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. Użytkownik rozpoczyna pracę w systemie informatycznym od następujących czynności:
   1) Włączenia komputera,
   2) Uwierzytelnienia się (logowania) w systemie informatycznym za pomocą swojego identyfikatora i hasła,
   3) Uwierzytelnienia się (logowania) w ramach bazy danych.
3. Niedopuszczalne jest logowanie się z wykorzystaniem identyfikatora i hasła innego użytkownika.
4. Przy opuszczaniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy uniemożliwić osobom nieuprawnionym dostęp do Systemu Informatycznego, np. poprzez zastosowanie wygaszacza ekranu wymagającego podania hasła lub poprzez wylogowanie się z Systemu.

5. Zakończenie przez użytkownika pracy w systemie informatycznym następuje po wylogowaniu się z Systemu. Po zakończeniu pracy użytkownik zobowiązany jest zabezpieczyć swoje stanowisko pracy, w szczególności informatyczne nośniki danych, dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych oraz wyłączyć komputer, bądź pozamykać wszystkie otwarte bazy danych, pliki i aplikacje i zablokować konsolę.
6. W przypadku wystąpienia nieprawidłowości w mechanizmie uwierzytelniania się w systemie informatycznym oraz/lub bazie danych użytkownik niezwłocznie powiadamia o nich pracownika odpowiedzialnego za obsługę informatyczną.

6. PROCEDURA TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Administrator danych odpowiada za okresowe wykonanie kopii bezpieczeństwa danych gromadzonych w Systemie Informatycznym, przy pomocy przewidzianych przez System Informatyczny narzędzi.
2. Kopia zbioru danych jest tworzona na zewnętrznym, zabezpieczonym dysku - w cyklu codziennym.
3. Nośniki z backupem są okresowo sprawdzane pod kątem ich przydatności do odtworzenia danych.

7. SPOSÓB I CZAS PRZECHOWYWANIA NOŚNIKÓW INFORMACJI, W TYM KOPII INFORMATYCZNYCH ORAZ WYDRUKÓW

1. Za zewnętrzne nośniki danych uważa się:
    - dyskietki, dyskietki zip;
    - dyski CD-R, CD-RW, DVD-R, DVD-RW itp.;
    - twarde dyski wymienne;
    - taśmy magnetyczne;
    - komputery przenośne;
    - inne nośniki, służące do przechowywania danych i mogące być przenoszone niezależnie od sprzętu komputerowego.

2. Nieupoważnieni pracownicy nie mogą wykonywać kopii baz (zbiorów) danych oraz zapisywać – na informatycznych nośnikach danych – danych osobowych, w szczególności dokonywać kopii zapasowej całych zbiorów danych.
3. Dane osobowe w postaci elektronicznej, za wyjątkiem kopii bezpieczeństwa, mogą być wynoszone poza obszar przetwarzania danych osobowych tylko w przypadku zapisania ich na przeznaczonym do tego komputerze przenośnym i przez upoważnionych do tego pracowników lub współpracowników Zakładu.
4. Wymienne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w pomieszczeniach stanowiących obszar przetwarzania danych osobowych.
5. Po zakończeniu pracy przez użytkowników Systemu Informatycznego wymienne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w zamykanych szafach biurowych.
6. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do likwidacji, są pozbawiane przez administratora danych zapisu tych danych, a w przypadku, gdy nie jest to możliwe, są uszkadzane w sposób uniemożliwiający ich odczytanie.
7. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe przeznaczone do naprawy są pozbawiane przez administratora danych zapisu tych danych.
8. Fizycznej likwidacji zniszczonych lub niepotrzebnych informatycznych nośników danych z danymi osobowymi należy dokonywać w sposób uniemożliwiający odczyt danych osobowych.
9. Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.
10. Dostęp do wydruków z Systemu Informatycznego zawierających dane osobowe mają wyłącznie osoby do tego upoważnione.
11. Wydruki są przechowywane w miejscu uniemożliwiającym bezpośredni do nich dostęp osobom niepowołanym.

8. PROCEDURA I SPOSÓB ZABEZPIECZENIA PRZED OPROGRAMOWANIEM, KTÓREGO CELEM JEST NIEUPRAWNIONY DOSTĘP DO ZASOBÓW SYSTEMU INFORMATYCZNEGO ORAZ POSTĘPOWANIE W PRZYPADKU AWARII ZASILANIA

1. Na wszystkich komputerach (w tym także komputerach przenośnych) oraz serwerach zostało zainstalowane oprogramowanie antywirusowe oraz oprogramowanie zapobiegające nieuprawnionemu dostępowi do Systemu Informatycznego.
2. W przypadku stwierdzenia wystąpienia wirusa administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do podjęcia działań zmierzających do wykrycia źródła pojawienia się wirusa w Systemie Informatycznym, jego wyeliminowania, a jeśli jest to niemożliwe – do usunięcia zainfekowanego pliku.
3. Sprzęt komputerowy służący do przetwarzania danych osobowych jest wyposażony w urządzenia podtrzymujące zasilanie.
4. W przypadku wystąpienia przerw w dostawie energii elektrycznej administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do:
   - zakończenia trwających procesów;
   - zakończenia pracy sprzętu (np. komputera).
5. Po przywróceniu zasilania i upewnieniu się, że jest ono trwałe, administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do:
   - włączenia sprzętu komputerowego;
   - kontroli poprawności jego funkcjonowania i działania Systemu Informatycznego.
6. W przypadku stwierdzenia nieprawidłowości działania Systemu Informatycznego administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do niezwłocznego podjęcia czynności, związanych z usunięciem awarii, opisanych w punkcie 3 poniżej.

9. PROCEDURA USUWANIA AWARII SPRZĘTU LUB OPROGRAMOWANIA

1. W przypadku wystąpienia awarii Systemu Informatycznego pracownik lub współpracownik, który ją stwierdził zobowiązany jest do zgłoszenia faktu wystąpienia awarii administratorowi danych lub osobie odpowiedzialnej za obsługę informatyczną.
2. Administrator danych lub osoba odpowiedzialna za obsługę informatyczną zobowiązany jest do niezwłocznego podjęcia czynności zmierzających do usunięcia awarii np. poprzez wezwanie serwisu.
3. Po usunięciu awarii administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do:

- uruchomienia Systemu Informatycznego;
- kontroli poprawności jego funkcjonowania;
- kontroli integralności danych.

4. W przypadku stwierdzenia uszkodzenia danych zgromadzonych w Systemie, administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do otworzenia danych z ostatniej posiadanej kopii bezpieczeństwa (backup).
5. W przypadku gdy usunięcie awarii wymaga przekazania sprzętu komputerowego na zewnątrz, przed przekazaniem tego sprzętu administrator danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do usunięcia z dysków twardych wszystkich danych, po ich uprzednim skopiowaniu na inny nośnik. Jeśli z przyczyn technicznych jest to niemożliwe, osoba przekazująca sprzęt ze strony Kancelarii zobowiązana jest uzyskać od serwisanta protokół przyjęcia danych i zobowiązanie do zachowania ich poufności.

10. SPOSÓB REALIZACJI WYMOGU ZAPISANIA W SYSTEMIE INFORMATYCZNYM INFORMACJI O ODBIORCACH DANYCH

1. Aktualnie dane osobowe nie są udostępniane innym podmiotom, niż wynika to z przepisów prawa
2. W przypadku udostępniania danych osobowych w Systemie Informatycznym możliwe jest sporządzenie i wydrukowanie raportu, zawierającym następujące informacje:
   - identyfikatora osoby, której dane dotyczą;
   - odbiorcy danych;
   - zakresu udostępnienia danych osobowych;

- daty operacji udostępnienia.

11. SPOSÓB I CZAS PRZECHOWYWANIA NOŚNIKÓW INFORMACJI, W TYM KOPII INFORMATYCZNYCH ORAZ WYDRUKÓW

1. Dokumenty papierowe zawierające dane osobowe przechowywane są wyłącznie w specjalnie do tego celu przeznaczonych segregatorach, w szafach zamykanych na klucz.
2. Nieupoważnieni pracownicy nie mogą wykonywać kopii baz danych oraz zapisywać - na informatycznych nośnikach danych - danych osobowych, w szczególności dokonywać kopii zapasowej całych zbiorów danych.
3. Fizycznej likwidacji zniszczonych lub niepotrzebnych informatycznych nośników danych z danymi osobowymi należy dokonywać w sposób uniemożliwiający odczyt danych osobowych.
4. Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.

12. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMU INFORMATYCZNEGO ORAZ INFORMATYCZNYCH NOŚNIKÓW DANYCH

1. Przegląd i konserwacja Systemu Informatycznego oraz informatycznych nośników danych zawierających dane osobowe dokonywane są poprzez:
   a) sprawdzanie zgodności danych z dokumentami;
   b) analizę zgłaszanych uwag użytkowników.
2. Przeglądu i konserwacji Systemu Informatycznego dokonuje administrator danych, osoba odpowiedziana za obsługę informatyczną lub inny upoważniony pracownik. Dopuszczalne jest zlecenie/powierzenie przeglądów i konserwacji zbiorów danych wyspecjalizowanym podmiotom zewnętrznym na podstawie pisemnych umów.
3. Przekazywane na zewnątrz Informatyczne nośniki danych (komputery, dyski, laptopy), dla celów naprawy czy konserwacji, nie zawierają baz (zbiorów) danych osobowych.

13. ROZPOWSZECHNIANIE I ZARZĄDZANIE DOKUMENTEM

1. Treść niniejszej Instrukcji ma charakter informacji stanowiącej tajemnicę przedsiębiorstwa, zgodnie z art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2003 r. Nr 153, poz. 1503 ze zm.) oraz chronionej tajemnicą pracodawcy na zasadzie art. 100 § 2 pkt 4 Kodeksu pracy (t.j. Dz. U. z 2016 r., poz.1666 ze zm.). Wybrane elementy Instrukcji mogą zostać udostępnione partnerom po zawarciu stosownej umowy o zachowaniu poufności.
2. Za zarządzanie Instrukcją, w tym jej rozpowszechnianie, aktualizację, utrzymywanie spójności z innymi dokumentami, jest odpowiedzialny administrator danych.
3. Z treścią niniejszego dokumentu powinni być zapoznani wszystkie osoby upoważnione do przetwarzania danych osobowych.

Załącznik nr 2 do Polityki Ochrony Danych Osobowych[1]:

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których przetwarzane są dane osobowe

Lp.	Lokalizacja – adres i numer budynku	Numer pomieszczenia/ przeznaczenie	Uwagi
1			
2			
3			
4			
5			
6			
7			

[1] W ramach niniejszego załącznika należy wskazać wszystkie lokalizacje, w którym administrator danych przetwarzane dane osobowe w którymkolwiek ze zbiorów danych.

Załącznik nr 3
do Polityki Ochrony Danych Osobowych

.....

(imię i nazwisko)

.....

(stanowisko służbowe)

.....

(nazwa komórki organizacyjnej)

OŚWIADCZENIE

OSOBY PRZETWARZAJĄCEJ DANE OSOBOWE

Oświadczam, że zostałam zapoznana/zostałem zapoznany z obowiązującymi przepisami prawa i wewnętrznie obowiązującymi w Zakładzie Aktywności Zawodowej w Bydgoszczy oraz Polityką Ochrony Danych Osobowych.

.....

(miejscowość i data)

.....

(podpis osoby składającej oświadczenie)

Załącznik nr 4
do Polityki Ochrony Danych Osobowych

Zakład Aktywności Zawodowej

W Bydgoszczy

Bydgoszcz, dnia ..... r.

UPOWAŻNIENIE

DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 oraz art. 32 ust. 4 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, Zakład Aktywności Zawodowej w Bydgoszczy, jako Administrator Danych, upoważnia Panią/Pana

.....

(imię, nazwisko)

do przetwarzania danych osobowych w systemach informatycznych, jak i w formie papierowej, w zakresie niezbędnym do realizacji zadań związanych z wykonywanymi obowiązkami służbowymi na stanowisku ..... zgodnie z zakresem czynności, oraz powierzonych jednorazowo lub na stałe przez przełożonego.

Dla potrzeb realizacji zadań, upoważniam Panią/Pana do przetwarzania danych osobowych, z zachowaniem pełnej ich ochrony, przy zastosowaniu środków technicznych i organizacyjnych obowiązujących w Zakładzie Aktywności Zawodowej w Bydgoszczy.

Upoważnienie traci moc w przypadku zmiany stanowiska pracy, ustania zatrudnienia lub odwołania upoważnienia.

Osoba upoważniona jest obowiązana do zachowania w tajemnicy danych osobowych, o których dowiedziała się w związku z przetwarzaniem danych oraz sposobów ich zabezpieczenia. Obowiązek ten nie wygasa w związku z ustaniem zatrudnienia. Za przetwarzanie danych osobowych nie będąc do tego uprawnionym grozi odpowiedzialność karna (art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych) .

.....
(podpis pracodawcy)

Przyjmuję do wiadomości i stosowania, a także zobowiązuję się do zachowania danych osobowych w tajemnicy

.....

Załącznik nr 5
do Polityki Ochrony Danych Osobowych

UMOWA
O POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH
/wzór/

zawarta w dniu ..... r. w Bydgoszczy, między:

Miastem Bydgoszcz z siedzibą w Bydgoszczy (85-102), ul. Jezuicka 1, NIP: 9531011863, reprezentowanym przez ..... - Dyrektora Zakładu Aktywności Zawodowej w Bydgoszczy przy ul. Ludwikowo 3, 85-502 Bydgoszcz, na podstawie pełnomocnictwa WOA-I.0052.421.2014 z dnia 14.07.2014 r. **(„Administrator Danych"),** reprezentowaną przez:

a

.....,

zwaną dalej *(np. Dostawcą, Wykonawcą, Usługodawcą),*
łącznie zwane „Stronami".

§ 1

Powierzenie przetwarzania danych osobowych

1. W celu wykonania umowy z dnia ..... (dalej „Umowa"), Administrator Danych powierza „....." przetwarzanie danych osobowych w trybie art. 28 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", dalej „Rozporządzenie",
2. Przetwarzanie danych przez Wykonawcę obejmuje dane osobowe
   .....
   (należy określić kategorie osób, których dane dotyczą, np. pracowników, właścicieli nieruchomości)
   w zakresie: .....
   (należy wskazać rodzaj (zakres) danych osobowych określonych kategorii osób, których dane dotyczą np. imię, nazwisko, adres zamieszkania, nr Pesel, nr rachunku bankowego, nr telefonu, adres e-mail, wizerunek).
3. Wykonawca jest uprawniony do wykonywania, na powyższych danych osobowych, następujących operacji: *(należy określić właściwe operacje, np. zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie, łączenie, ograniczanie, usuwanie, niszczenie, inne).*

4. Przetwarzanie przez Wykonawcę powierzonych danych osobowych będzie trwało w okresie ..... *(np. od....do,.., realizacji Umowy).*
5. Wykonawca zobowiązuje się do przetwarzania powierzonych danych osobowych wyłącznie w celu i zakresie oraz w sposób i przez czas określony w ust. 1-4 .
6. Wykonawca oświadcza, że nie będzie przetwarzał powierzonych danych osobowych w państwie trzecim, tj. w państwie nienależącym do Europejskiego Obszaru Gospodarczego.

§ 2

Zasady przetwarzania powierzonych danych osobowych

1. Wykonawca zobowiązuje się wykonać wszelkie czynności wynikające z Umowy o powierzenie i przepisów o ochronie danych osobowych z najwyższą starannością.
2. W przypadku wystąpienia zagrożeń mogących mieć wpływ na odpowiedzialność Administratora Danych za przetwarzanie powierzonych danych osobowych, Wykonawca zobowiązuje się niezwłocznie podjąć działania w celu ich usunięcia oraz natychmiast zawiadomić o nich Administratora Danych.
3. Administrator Danych wyraża zgodę na ewentualne dalsze powierzenie przetwarzania danych osobowych, przez Wykonawcę innemu podmiotowi przetwarzającemu. Dalsze powierzenie może nastąpić na podstawie pisemnej umowy, na mocy której zostaną nałożone te same obowiązki, jak w niniejszej Umowie o powierzenie. O zamiarze dalszego powierzenia Wykonawca każdorazowo poinformuje Administratora Danych.
4. W przypadku niewyrażenia przez Administratora Danych sprzeciwu w terminie . . . . . dni od dnia otrzymania informacji przez Administratora Danych umowa może zostać zawarta. Po zawarciu umowy Wykonawca jest zobowiązany poinformować o tym fakcie Administratora Danych podjąć dane podmiotu, któremu powierzył przetwarzanie danych. W przypadku nie wywiązania się przez inny podmiot przetwarzający ze spoczywających na nim obowiązków ochrony danych osobowych, pełną odpowiedzialność wobec Administratora Danych za ich wypełnienie ponosi Wykonawca.

§ 3

Zabezpieczenie powierzonych danych osobowych

1. Wykonawca zapewnia, że wdroży odpowiednie środki techniczne i organizacyjne, aby przetwarzanie spełniało wymogi określone w obowiązujących przepisach prawa i chroniło prawa osób, których dane dotyczą.
2. Wykonawca oświadcza, że posiada niezbędną wiedzę w zakresie przetwarzania danych osobowych, wiarygodność oraz zasoby do należytego wykonania niniejszej Umowy.
3. Wykonawca zobowiązuje się w szczególności do:
   a. przetwarzania danych wyłącznie na udokumentowane polecenie Administratora Danych; za udokumentowane polecenie uznaje się zadania nałożone na Wykonawcę w Umowie;
   b. podjęcia wszelkich środków, aby zapewnić bezpieczeństwo przetwarzania danych osobowych zgodnie z wymogami nałożonymi na mocy art. 32 Rozporządzenia;
   c. dopuszczenia do przetwarzania danych osobowych wyłącznie osób posiadających wydane przez niego upoważnienie i zapoznanych przez niego z przepisami o ochronie danych osobowych;
   d. zapewnienia, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania danych osobowych w tajemnicy;

e. pomagania Administratorowi Danych poprzez odpowiednie środki techniczne i organizacyjne wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale 3, a także z obowiązków określonych w art. 32-36 Rozporządzenia;

f. udostępniania Administratorowi Danych wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia;

g. prowadzenia rejestru kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 Rozporządzenia, jeżeli jest wymagane na mocy Rozporządzenia.

4. Wykonawca zobowiązuje się bez zbędnej zwłoki zgłosić Administratorowi Danych:
   a. stwierdzenie naruszenia ochrony danych osobowych, nie później niż w ciągu 24 godzin od stwierdzenia naruszenia, zawierające co najmniej informacje, o których mowa w art. 33 ust. 3 Rozporządzenia;
   b. otrzymanie żądania od osoby, której dane przetwarza, w zakresie przetwarzania dotyczących jej danych osobowych;
   c. wszczęcie u Wykonawcy, przez organ właściwy ds. ochrony danych osobowych, kontroli sposobu przetwarzania powierzonych danych osobowych.

§ 4

Nadzór nad wykonaniem Umowy o powierzenie

1. Administrator Danych jest uprawniony do audytu wykonywania przez Wykonawcę obowiązków określonych w niniejszej Umowie o powierzenie.
2. Wykonawca umożliwia Administratorowi Danych lub audytorowi upoważnionemu przez Administratora Danych przeprowadzenie audytów, w tym inspekcji. W szczególności Wykonawca:
   a. zapewni wstęp do pomieszczeń, w których Wykonawca przetwarza powierzone dane osobowe;
   b. przekaże pisemne lub ustne wyjaśnienia w celu ustalenia stanu faktycznego;
   c. umożliwi przeprowadzenie oględzin dokumentów a także urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.
3. Z czynności sporządza się protokół, którego jeden egzemplarz doręcza się kontrolowanemu.
4. W przypadku stwierdzenia uchybień w zakresie wykonywania Umowy o powierzenie lub przepisów o ochronie danych osobowych, Administratorowi Danych przysługuje prawo do żądania natychmiastowego wstrzymania przetwarzania danych osobowych i wyznaczenia Wykonawcy terminu na usunięcie uchybień.

§ 5

Odpowiedzialność Wykonawcy

Wykonawca zobowiązuje się do naprawienia szkody wyrządzonej Administratorowi Danych w wyniku naruszenia danych osobowych z winy Wykonawcy. W szczególności zobowiązuje się do pokrycia kar zapłaconych przez Administratora Danych, poniesionych przez Administratora Danych, kosztów procesu i zastępstwa procesowego, a także odszkodowania na rzecz osoby, której naruszenie dotyczyło.

§ 6

Wygaśnięcie Umowy

1. Umowa o powierzenie zostaje zawarta na okres od dnia .....do dnia.....
2. Po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych, Wykonawca zobowiązuje się niezwłocznie, nie później niż w terminie ..... dni (do decyzji Administratora Danych) usunąć lub zwrócić Administratorowi Danych wszelkie dane osobowe oraz skutecznie usunąć wszelkie istniejące kopie, chyba że przepisy prawa nakazują przechowywanie danych. Z czynności usunięcia lub zwrotu należy sporządzić pisemny protokół. Powierzenie trwa do czasu wykonania tych czynności.

§ 7

Postanowienia końcowe

1. Wszelkie zmiany i uzupełnienia Umowy o powierzenie dokonywane będą w formie pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych zastosowanie znajdują przepisy o ochronie danych osobowych.
3. W przypadku sporów wynikających z realizacji Umowy o powierzenie Strony poddają jej rozstrzygnięciu przez sąd właściwy ze względu na siedzibę Administratora Danych.
4. Umowa została sporządzona w ..... jednobrzmiących egzemplarzach, ... egz. dla Administratora Danych, ... egz. dla Wykonawcy.

....

Administrator Danych Wykonawca

Załącznik nr 6
do Polityki Ochrony Danych Osobowych

RAPORT

Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Data wykrycia naruszenia:

   .....

2. Nazwa komórki, w której nastąpiło zdarzenie:

   .....

3. Krótki opis zaistniałej sytuacji:

   .....

   .....

   .....

4. Rodzaj i zakres informacji, których ochrona została naruszona:

   .....

5. Działania podjęte w związku ze zdarzeniem:

   .....

   .....

   .....

.....
Data i podpis osoby sporządzającej raport

Załącznik nr 7

do Polityki Ochrony Danych

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

Dane Administratora danych osobowych:

Dane kontaktowe osoby odpowiedzialnej/Inspektora Ochrony Danych:

Lp	Nazwa zbioru	Opis zbioru	Miejsce/Program	Kategorie odbiorców	Pola informacyjne	Cel przetwarzania	Kategoria przetwarzanych danych osobowych	Termin usunięcia danych	Zastosowane środki bezpieczeństwa
1									
2									
3									
4									

Załącznik nr 8
do Polityki Ochrony Danych Osobowych

Ewidencja osób upoważnionych do przetwarzania danych osobowych[1]

Lp.	Nazwisko	Imię	Identyfikator [2]	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						

[1] Tabela do uzupełnienia w zakresie osób w sferze wewnętrznej Zakładu (pracownicy, współpracownicy), którym wydano imienne pisemne upoważnienie do przetwarzania danych osobowych. Zakres upoważnienia wpisany w ewidencji powinien się zgadzać z zakresem wynikającym z pisemnego upoważnienia do przetwarzania danych osobowych.
[2] Identyfikator należy wskazać w przypadku przetwarzania danych w systemie informatycznym przez daną osobę upoważnioną

Załącznik nr 9
do Polityki Ochrony Danych Osobowych

Wykaz zbiorów danych i systemów zastosowanych do ich przetwarzania[1]

Lp.	Nazwa zbioru danych osobowych	System zastosowany do przetwarzania /nazwa systemu informatycznego/[2]	Zakres danych osobowych w zbiorze danych /kategorie danych/[3]	Komunikacja z innymi systemami[4] (T/N)	Przepływ danych[5]
1.	Zbiór danych klientów		• Imiona i nazwiska • Miejsce urodzenia • Adres zamieszkania lub pobytu • Numer telefonu • Adres e-mail •		
2.	Zbiór danych pracowników i współpracowników		• Imiona i nazwiska • Imiona rodziców • Data i miejsce urodzenia • Miejsce zamieszkania lub pobytu • Wykształcenie, zawód, miejsce pracy • PESEL • Numer telefonu • Adres e-mail • Numer rachunku bankowego • ..... •		

[1] Przedstawiony załącznik zawiera przykładowy wykaz przetwarzanych zbiorów. Każdorazowo należy zweryfikować, czy wszystkie te zbiory występują u danego administratora.
[2] Jeżeli dane nie są przetwarzane w dedykowanym systemie informatycznym, można wskazać przykładowo: *Dane w postaci dokumentów Word, PDF, Dane w postaci papierowej, Wykaz w postaci arkusza kalkulacyjnego.*
[3] Należy wskazać szczegółowo kategorie danych przetwarzanych w zbiorze. Przykładowo:
1. Imię (imiona) i nazwisko
2. Data urodzenia
3. Adres zamieszkania
4. Nr ewidencyjny PESEL
5. Miejsce pracy
6. Zawód
7. Wykształcenie
8. Dowód osobisty
9. Numer telefonu
10. Adres poczty elektronicznej

[4] Należy wskazać, czy dany system komunikuje się z innymi systemami, którymi dysponuje administrator danych.
[5] Należy wskazać sposób współpracy pomiędzy różnymi systemami informatycznymi oraz relacje, jakie istnieją pomiędzy danymi zgromadzonymi w zbiorach, do przetwarzania których systemy są wykorzystywane. W opisie przepływu danych należy umieścić, czy ten przepływ jest jedno- (np. dane przez system informatyczny są pobierane tylko do odczytu) czy dwukierunkowy (np. dane są pobierane do odczytu i zapisu). W opisie przepływu danych należy również wskazać, czy są one przenoszone manualnie (przy wykorzystaniu zewnętrznych nośników danych), półautomatycznie (np. za pomocą teletransmisji wykorzystując funkcje eksportu/importu danych).

Załącznik nr 10

do Polityki Ochrony Danych Osobowych

REJESTR POWIERZEŃ PRZETWARZANIA DANYCH OSOBOWYCH

LP.	Nazwa podmiotu (powierzającego lub podmiotu przetwarzającego)	Lokalizacja umowy	Data nadania umowy	Dane kontaktowe osób opiniujących umowę po stronie kontrahenta	Data otrzymania ostatniej odpowiedzi od kontrahenta	Status umowy