Polityka Bezpieczeństwa przetwarzania danych osobowych

Rozdział 1
Postanowienia ogólne

§ 1.

Polityka Bezpieczeństwa przetwarzania danych osobowych, zwana dalej „Polityką", określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w zbiorach w Miejsko-Gminnym Ośrodku Kultury w Woźnikach, ul. Górna 5, zwanym dalej „ADO".

§ 2.

Użyte w Polityce określenia oznaczają:	
Administrator Danych (ADO)	Dyrektor Miejsko-Gminnego Ośrodka Kultury w Woźnikach, ul. Górna 5
Rozporządzenie (RODO)	ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
użytkownik	- osobę upoważnioną do przetwarzania danych osobowych;
naruszenie zabezpieczenia	- jakiekolwiek naruszenie bezpieczeństwa, niezawodności, integralności lub poufności;
dane osobowe	- wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
przetwarzanie danych osobowych	- jakiekolwiek operacje wykonywane na danych osobowych polegające na: zbieraniu, utrwalaniu, opracowywaniu, zmienianiu, przechowywaniu, analizowaniu, raportowaniu, aktualizowaniu, udostępnianiu lub usuwaniu danych osobowych;
usuwanie danych osobowych	- zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
zbiór danych osobowych	- posiadający strukturę zestaw danych o charakterze danych osobowych, które są dostępne według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
zabezpieczenie danych osobowych	- środki administracyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, nieuprawnionym dostępem i modyfikacją, ujawnieniem lub pozyskaniem danych osobowych bądź ich utratą;
Instrukcja	- Instrukcję Zarządzania Systemem Informatycznym
Pracownik	- osobę zatrudnioną na podstawie stosunku pracy lub innego stosunku prawnego;

Rozdział 2
Zakres oraz zasady zabezpieczania danych osobowych

§ 3.

Niniejszą politykę stosuje się do zbiorów danych osobowych znajdującego się u ADO.

§ 4.

Nadzór ogólny nad realizacją przepisów wynikających z ustawy oraz rozporządzenia pełni ADO. Nadzór nad poprawnością realizacji przepisów o ochronie danych osobowych, w szczególności zasad opisanych w Polityce oraz Instrukcji, oraz nad wykonywaniem zadań związanych z ochroną danych osobowych IODO.

§ 5.

Dane osobowe przetwarzane podlegają ochronie zgodnie z przepisami ustawy.

§ 6.

Przetwarzanie danych osobowych jest dopuszczalne wyłącznie w zakresie niezbędnym.

§ 7.

Przetwarzanie danych osobowych nie może naruszać praw i wolności osób, których dane osobowe dotyczą, a w szczególności zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

§ 8.

W przypadku zbierania jakichkolwiek danych osobowych bezpośrednio od osoby, której dane dotyczą, osoba zbierająca dane osobowe jest zobowiązana do przekazania tej osobie informacji m.in. o:
- pełnej nazwie ADO oraz jego adresie;
- celu zbierania danych osobowych;
- prawie dostępu do treści swoich danych osobowych oraz ich poprawiania;
- dobrowolności podania danych osobowych, z zastrzeżeniem, że odmowa zgody na ich przetwarzanie skutkuje niemożnością świadczenia usług

§ 9.

Jakiekolwiek udostępnianie danych osobowych może odbywać się wyłącznie w trybie określonym w RODO oraz w pełnej zgodności z przepisami prawa. Wnioski o udostępnienie danych osobowych przetwarzanych, po wstępnym rozpatrzeniu przez IODO, są rozpatrywane przez ADO.

§ 10.

Przetwarzanie danych osobowych może zostać powierzone innemu podmiotowi, wyłącznie w celu określonym w § 6, pod warunkiem zawarcia z tym podmiotem pisemnej umowy lub porozumienia, w pełni respektujących przepisy RODO, w zakresie dotyczącym zasad przetwarzania danych osobowych, zaopiniowane przez IODO.

§ 11.

Każdej osobie, której dane osobowe są przetwarzane przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności m.in. prawo do:
- uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby ADO;
- uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
- uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;
- uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
- uzyskania informacji o profilowaniu;
- uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
- żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.

§ 12.

Na wniosek osoby, której dane osobowe dotyczą, ADO jest zobowiązany, w terminie maksymalnie 30 dni od dnia wpłynięcia wniosku, wskazać m.in. w powszechnie zrozumiałej formie:
- jakie dane osobowe dotyczące zapytującej osoby są przetwarzane przez ADO;
- w jaki sposób zebrano te dane osobowe;
- w jakim celu i zakresie te dane osobowe są przetwarzane;
- od kiedy są przetwarzane te dane osobowe;
- w jakim zakresie oraz komu te dane osobowe zostały udostępnione.

§ 13.

W razie wykazania przez osobę, której dane osobowe dotyczą, że jej dane osobowe, przetwarzane są niekompletne, nieaktualne, nieprawdziwe, lub zostały zebrane z naruszeniem RODO albo są zbędne do realizacji celu, w jakim zostały zebrane, ADO jest zobowiązany do uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych osobowych lub ich usunięcia, zgodnie z żądaniem osoby, której dane osobowe dotyczą.

Rozdział 3
Obowiązki ADO

§ 14.

IODO poza realizacją zadań wynikających z Polityki, sprawuje ogólny nadzór nad realizacją czynności dotyczących przetwarzania danych osobowych.

§ 15.

Do zadań IODO należy w szczególności:
- współdziałanie z ADO w zakresie zapewniającym wypełnianie przez ADO obowiązków wynikających z RODO;
- prowadzenie i aktualizacja rejestru, o którym mowa w § 20, który stanowi załącznik nr 1 do Polityki;
- prowadzenie i aktualizacja wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, który stanowi załącznik nr 2 do Polityki;

- analiza i identyfikacja zagrożeń i ryzyka, na które może być narażone przetwarzanie danych osobowych w ramach oraz pisemne informowanie o wynikach analizy osoby upoważnione do podejmowania decyzji;
- opiniowanie umów, których przedmiotem jest powierzenie przetwarzania danych osobowych w podmiotowi zewnętrznemu wobec ADO;
- inicjowanie szkoleń osób zajmujących się przetwarzaniem oraz ochroną danych osobowych.

§ 16.

W doborze i stosowaniu środków ochrony danych osobowych IODO zwraca szczególną uwagę na ich należyte zabezpieczenie przed udostępnieniem osobom nieuprawnionym, kradzieżą, uszkodzeniem lub nieuprawnioną modyfikacją.

§ 17.

Obowiązki IODO wykonywane są przez wyznaczonego przez osobę upoważnioną do podejmowania decyzji w imieniu ADO.

§ 18.

W razie konieczności, w kwestiach związanych z zastosowaniem środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych IODO konsultuje się i współpracuje z innymi IODO w podmiotach zewnętrznych.

Rozdział 4
Przetwarzanie danych osobowych

§ 19.

Do przetwarzania danych osobowych w mogą być dopuszczeni jedynie pracownicy posiadający odpowiednie upoważnienie wydane przez upoważnioną do tego osobę.
Każdy pracownik, przed dopuszczeniem go do przetwarzania danych osobowych, musi być zapoznany z przepisami dotyczącymi ochrony danych osobowych oraz Polityką i Instrukcją.
Pracownik potwierdza zapoznanie się z przepisami dotyczącymi ochrony danych osobowych oraz Polityką i Instrukcją przez złożenie podpisu na liście prowadzonej przez IODO, której wzór jest określony w załączniku nr 3 do Polityki.

§ 20.

Każdy pracownik mający dostęp do danych osobowych jest wpisywany do rejestru osób upoważnionych do przetwarzania danych osobowych, prowadzonego przez IODO.
Rejestr, o którym mowa w ust. 1, zawiera:
- imię i nazwisko pracownika;
- jego identyfikator w systemie informatycznym służącym przetwarzaniu danych;
- zakres przydzielonego uprawnienia;
- datę przyznania uprawnień;
- podpis IODO potwierdzający przyznanie uprawnień;
- datę odebrania uprawnień;
- podpis IODO potwierdzający odebranie uprawnień.

§ 21.

Dopuszczenie do przetwarzania danych osobowych przez osoby niebędące pracownikami, jest możliwe tylko w wyjątkowych przypadkach, po uzyskaniu pozytywnej opinii IODO oraz podpisaniu z tą osobą umowy zapewniającej przestrzeganie przepisów dotyczących ochrony

danych osobowych. W takim przypadku § 19 i 20 stosuje się odpowiednio. Osoby trzecie mogą przebywać na obszarze, w którym są przetwarzane dane osobowe jedynie w obecności co najmniej jednego użytkownika odpowiedzialnego za te osoby.

§ 22.

Wszyscy pracownicy oraz osoby, o których mowa w § 21 ust. 1, pod groźbą sankcji dyscyplinarnych, mają obowiązek zachowania tajemnicy o przetwarzanych u ADO danych osobowych oraz o stosowanych sposobach zabezpieczeń danych osobowych. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia lub współpracy.

§ 23.

Użytkownicy są w szczególności zobowiązani do:
- bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji, określonych w Polityce, Instrukcji i innych procedurach, dotyczących zarządzania oraz jego obsługi;
- przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych (lub wyznaczonych ich częściach);
- zabezpieczania zbioru danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce, Instrukcji i innych procedurach dotyczących zarządzania oraz jego obsługi;
- niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie;
- nieudzielania informacji o danych osobowych przetwarzanych innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;
- bezzwłocznego zawiadamiania IODO o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe.

§ 24.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych są określone w załączniku nr 4 do Polityki.

Rozdział 5
Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 25.

Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:
- stwierdzono naruszenie zabezpieczenia;
- stan sprzętu komputerowego, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych;
- inne okoliczności wskazują, że mogło nastąpić nieuprawnione udostępnienie danych osobowych przetwarzanych.

§ 26.

Każdy użytkownik, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, jest zobowiązany do niezwłocznego poinformowania o tym bezpośredniego przełożonego oraz IODO, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych jest zobowiązany niezwłocznie:
- poinformować pisemnie o zaistniałym zdarzeniu IODO i stosować się do jego zaleceń;

- zapisać wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnego wykrycia tego faktu.
- IODO, który stwierdził lub uzyskał informację wskazującą na naruszenie zabezpieczenia systemu informatycznego służącego przetwarzaniu danych osobowych jest zobowiązany niezwłocznie:
- wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzyć je datą i podpisać;
- przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym określić skalę zniszczeń, metody dostępu osoby niepowołanej do danych osobowych w systemie informatycznym służącym przetwarzaniu danych osobowych;
- podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć przed usunięciem ślady naruszenia ochrony danych osobowych, w szczególności przez:
- fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobowych osobie niepowołanej,
- wylogowanie użytkownika podejrzanego o naruszenie ochrony danych osobowych,
zmianę hasła użytkownika, przez którego uzyskano nielegalny dostęp do danych osobowych w celu uniknięcia ponownej próby uzyskania takiego dostępu;
- szczegółowo analizować stan systemu informatycznego służącego przetwarzaniu danych osobowych w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych;
- przywrócić normalne działanie systemu informatycznego służącego przetwarzaniu danych osobowych.

§ 27.

Po przywróceniu normalnego stanu należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości. Jeżeli przyczyną zdarzenia był błąd użytkownika, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych osobowych.
Jeżeli przyczyną zdarzenia była infekcja wirusem lub innym niebezpiecznym oprogramowaniem, należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne, wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika należy wyciągnąć konsekwencje dyscyplinarne wynikające z przepisów prawa pracy oraz wewnętrznych uregulowań ADO, a w przypadku gdy użytkownik nie jest pracownikiem, konsekwencje wynikające z umowy, o której mowa w § 21 ust. 1.

§ 28.

IODO przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach z naruszenia zabezpieczenia i w terminie niezwłocznym od daty powzięcia wiedzy o naruszeniu zabezpieczenia przekazuje go ADO.
Jeżeli naruszenie zabezpieczenia nastąpiło na skutek naruszenia zabezpieczeń systemu informatycznego służącego do przetwarzania danych IODO przygotowując raport, o którym mowa w ust. 1 współpracuje z Administratorem Systemu Informatycznego, o ile został powołany.

Rozdział 6
Kontrola nad przestrzeganiem ochrony danych osobowych

§ 29.

Bieżąca kontrola nad przetwarzaniem danych osobowych jest dokonywana przez IODO.
W ramach kontroli, o której mowa w ust. 1 IODO jest zobowiązany do nadzorowania, przestrzegania przez użytkowników wymagań Polityki i Instrukcji.

§ 30.

IODO przeprowadza w pierwszym kwartale roku kalendarzowym kontrolę w zakresie przestrzegania przez użytkowników Polityki, Instrukcji oraz innych przepisów prawa w zakresie ochrony danych osobowych, z czego sporządza odpowiedni raport. Przygotowując raport, o którym mowa w ust. 1, IODO uwzględnia informacje zawarte w raportach, o których mowa w § 28.

§ 31.

Kontrola, o której mowa w § 30, polega w szczególności na sprawdzeniu:
- którzy pracownicy mają dostęp do danych osobowych;
- czy dane osobowe nie zostały udostępnione nieupoważnionym pracownikom lub osobom;
- czy pracownicy i inne osoby mające dostęp do danych osobowych przetwarzanych - posiadają odpowiednie upoważnienia do przetwarzania danych osobowych wydane przez upoważnioną do tego osobę.

Rozdział 7
Postanowienia końcowe

§ 32.

Polityka jest dokumentem wewnętrznym ODO i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

§ 33.

Do spraw nieuregulowanych w Polityce stosuje się przepisy o ochronie danych osobowych RODO.

§ 34.

Polityka nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia.

§ 35.

Wykazy i rejestry znajdujące się w załącznikach do Polityki, prowadzi IODO.

§ 36.

Integralną część niniejszej Polityki stanowią następujące załączniki:
Załącznik nr 1 – Rejestr osób upoważnionych do przetwarzania danych osobowych;
Załącznik nr 2 – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe;
Załącznik nr 3 – Lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych;
Załącznik nr 4 – Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych;
Załącznik nr 5 – Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
Załącznik nr 6 - Wykaz programów zastosowanych do przetwarzania danych osobowych

Załącznik nr 1 do Polityki Bezpieczeństwa
Rejestr osób upoważnionych do przetwarzania danych osobowych.

Lp.	**Imię i nazwisko**	**Zakres przydzielonych uprawnień**	**Data przyznanych uprawnień**	**Podpis IODO**	**Data odebrania uprawnień**	**Podpis IODO**
1.						
2.						
3.						
4.						
5.						

Załącznik nr 2 do Polityki Bezpieczeństwa

Wykaz budynków, tworzących obszar, w którym są przetwarzane dane osobowe.

Lp.	**Budynek - nazwa**	**Dane adresowe**
1.	Miejsko-Gminny Ośrodek Kultury w Woźnikach	42-289 Woźniki, ul. Górna 5
2.	Filia Miejsko-Gminnego Ośrodka Kultury w Psarach	42-287 Psary, ul. Główna 89

Załącznik nr 3 do Polityki Bezpieczeństwa

Lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych.
Oświadczam, iż zapoznałem/am się z:
przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz przepisami wykonawczymi do niniejszej ustawy, Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/676 z dnia 27 kwietnia 2016 r. oraz Polityką Bezpieczeństwa.

Lp.	**Imię i nazwisko**	**Data**	**Podpis potwierdzający zapoznanie się z ww. dokumentami**
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			

Załącznik nr 4 do Polityki Bezpieczeństwa

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych

I. Środki ochrony fizycznej danych:

Klucze do pomieszczeń wydawane wyłącznie osobom upoważnionym, podczas nieobecności osób uprawnionych pomieszczenia, w których są przetwarzane dane osobowe są zamykane na klucz, urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych, pozbawia się wcześniej zapisu tych danych, zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej szafie, kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętej szafie, dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

II. Środki sprzętowe, informatyczne i telekomunikacyjne:

Sieć komputerowa jest zabezpieczona przed nieuprawnionym dostępem z sieci Internet poprzez zastosowanie firewalla programowego chroniącego zasoby beneficjenta. Oprogramowanie antywirusowe działające w czasie rzeczywistym na wszystkich komputerach wykrywa i eliminuje wirusy, konie trojańskie, robaki komputerowe oprogramowanie szpiegujące i kradnące hasła oraz inne niebezpieczne oprogramowanie. Dostęp do systemu operacyjnego komputera, w którym są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. Zainstalowano wygaszacze ekranów na stanowiskach, na których są przetwarzane dane osobowe.

III Środki organizacyjne:

Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych. Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zobowiązane do zachowania ich w tajemnicy. Monitory komputerów, na których są przetwarzane dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane. Kopie zapasowe zbioru danych osobowych są przechowywane w innym pomieszczeniu niż to, w którym znajduje się komputer, na którym dane osobowe są przetwarzane na bieżąco.

Załącznik nr 5 do Polityki Bezpieczeństwa

Wykaz wewnętrznych zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Lp.	Zbiór danych	Nazwa programu
1.	Dane osobowe pracowników	PROGMAN KADRY
2.	Dane osobowe pracowników	PROGMAN PŁACE
3.	Dane osobowe pracowników	PŁATNIK do ZUS
4.	Dane osób zatrudnionych na umowę zlecenia	PROGMAN ZLECONE

Załącznik nr 6 do Polityki Bezpieczeństwa
Programy zastosowane do przetwarzania danych osobowych:

- Microsoft Office
- Open Office
- Progman Kadry
- Progman Płace
- Progman Zlecone
- Płatnik do ZUS