POLITYKA BEZPIECZEŃSTWA
I REGULAMIN
OCHRONY DANYCH OSOBOWYCH
w Zespole Szkół Technicznych
im. gen. Władysława Andersa
w Białymstoku

AdministratorBezpieczeństwa Informacji

Białystok, 2014r.

S P I S T R E Ś C I

I. POLITYKA BEZPIECZEŃSTWA

A. POJĘCIA PODSTAWOWE

1. Polityka Bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2014 r. poz. 1182) oraz rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024). Opracowany dokument jest zgodny z dyrektywą 2002/58/WE Parlamentu Europejskiego i Radyz dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej.
2. Regulamin niniejszy określa tryb i zasady ochrony danych osobowych przetwarzanychw Zespole Szkół Technicznych im. gen. Władysława Andersa w Białymstoku, zwanym dalej Szkołą.
3. Ilekroć w regulaminie jest mowa o:
   a) **Szkole**–rozumie się przez to **Zespół Szkół Technicznych im. gen. Władysława Andersa w Białymstoku**;
   b) **zbiorze danych osobowych**–rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
   c) **danych osobowych**–rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
   d) **przetwarzaniu danych**–rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
   e) **systemie informatycznym**–rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
   f) **systemie tradycyjnym**–rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe w celu przetwarzania danych osobowych na papierze;
   g) **zabezpieczeniu danych w systemie informatycznym**–rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

h) **usuwaniu danych**–rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

i) **administratorze danych osobowych**–w świetle art. 3 i 7 pkt 4 ustawy o ochronie danych osobowych rozumie się przez to Dyrektora Szkoły, który decyduje o celach i środkach przetwarzania danych osobowych;

j) **administratorze bezpieczeństwa informacji**–rozumie się przez to osobę wyznaczoną przez Dyrektora Szkoły, nadzorującą przestrzeganie zasad ochrony danych osobowych, w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem danychoraz upoważnioną do realizacji zadań związanych z zarządzaniem systemem informatycznym;

k) **użytkowniku systemu informatycznego**–rozumie się przez to upoważnionego przez Dyrektora Szkoły, wyznaczonego do przetwarzania danych osobowych w systemie informatycznym pracownika, który odbył stosowne szkolenie w zakresie ochrony tych danych;

l) **zgodzie osoby, której te dane dotyczą**–rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie.Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.

B. CELE

Celem opracowania polityki bezpieczeństwa jest ochrona przed niepowołanym dostępem do:

a) systemu informatycznego oraz informacji udostępnianych z jego wykorzystaniem;

b) informacji zgromadzonych, przetwarzanych w formie tradycyjnej.

Niniejsze opracowanie określa politykę bezpieczeństwa w zakresie przetwarzania danych osobowych przez pracowników Szkoły, a w szczególności Administratora Danych Osobowych oraz Administratora Bezpieczeństwa Informacji.

Dane osobowe w Szkole są gromadzone, przechowywane, edytowane, archiwizowane w kartotekach, skorowidzach, księgach, wykazach, zestawieniach oraz w innych zestawach i zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Szkoły na dokumentach papierowych, jak również w systemach informatycznych na elektronicznych nośnikach informacji.

Powyższy dokument wprowadza regulacje w zakresie zasad organizacji procesu przetwarzania i odnosi się swoją treścią do informacji:

a) w formie papierowej przetwarzanej w ramach SYSTEMU TRADYCYJNEGO;

b) wformieelektronicznej

przetwarzanejwramachSYSTEMUINFORMATYCZNEGO;

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują Administratorzy Danych Osobowych.

Z zapisanymi w polityce bezpieczeństwa obowiązkowo są zapoznawani wszyscy użytkownicy systemów informatycznych i tradycyjnych.

Do informacji przechowywanych w systemach informatycznych jak i dokumentów tradycyjnych mają dostęp jedynie upoważnieni pracownicy Szkoły oraz osoby mające imienne zarejestrowane upoważnienie. Wszyscy pracownicy zobowiązani są do zachowania tych danych w tajemnicy. Dopuszczalny sposób i zakres przetwarzania danych osobowych regulują zapisy ustaw kompetencyjnych, szczegółowych właściwych dla komórek organizacyjnych Szkoły.

Dane osobowe są chronione zgodnie z polskim prawem oraz procedurami obowiązującymi w instytucjach samorządowych dotyczącymi bezpieczeństwa i poufności przetwarzanych danych. Systemy informatyczne oraz tradycyjne, które przechowują dane osobowe, są chronione odpowiednimi środkami technicznymi. Opracowane procedury określają obowiązki użytkownika zbiorów tradycyjnych oraz zasady korzystania z systemów informatycznych. Każdy użytkownik systemu informatycznego zobowiązany jest zapamiętać swoją nazwę użytkownika oraz hasło i nie udostępniać go innym osobom. Użytkownik systemu informatycznego powinien pamiętać o wylogowaniu się po zakończeniu korzystania z usług systemów informatycznych.

II. ADMINISTRACJA I ORGANIZACJA BEZPIECZEŃSTWA

A. INFORMACJE OGÓLNE

Za bezpieczeństwo danych osobowych przetwarzanych w systemach przetwarzania danych osobowych odpowiada Administrator Danych Osobowych. Administrator Danych Osobowych obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, awszczególności powinni zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem znaruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem danych.

Administrator Danych Osobowych wyznacza Administratora Bezpieczeństwa Informacji, nadzorującego przestrzeganie zasad ochrony. Imienne upoważnienie udzielane jest w formie pisemnej i stanowi załącznik nr 1 do niniejszego regulaminu.

Administrator Danych Osobowych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych. Prowadzi również ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:

a) imię, nazwisko i stanowisko osoby upoważnionej,

b) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych lub nazwę użytkowanego programu (aplikacji).

Upoważnienie do przetwarzania danych osobowych wydawane przez Administratora Danych Osobowych pracownikom Szkoły stanowi załącznik nr 2, a ewidencję osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 4 do niniejszego regulaminu.

Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia. Oświadczenie o zapewnieniu ochrony danych osobowych stanowi załącznik nr 3 do niniejszego regulaminu.

B. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

Administrator Bezpieczeństwa Informacji wykonuje wszystkie prace niezbędne do efektywnego oraz bezpiecznego zarządzania systemami informatycznymi i tradycyjnymi.

Administrator Bezpieczeństwa Informacji jest zobowiązany do zapewnienia, poprzez zastosowanie odpowiednich środków i metod kontroli dostępu, iż wyłącznie autoryzowany personel ma dostęp do systemów informatycznych i tradycyjnych. Ponadto, w uzgodnieniu z Administratorem Danych Osobowych, przydziela użytkownikom systemu informatycznego konta i hasła oraz określa warunki i sposób ich przydzielania. Administrator Bezpieczeństwa Informacji posiada bieżącą listę osób upoważnionych do przetwarzania danych osobowych.

Szczegółowy zakres odpowiedzialności i obowiązków Administratora Bezpieczeństwa Informacji obejmuje:

a) nadzorowanie bezpieczeństwa systemów informatycznych i tradycyjnych;

b) zapewnianie aktualizacji oprogramowania i dokumentacji technicznej systemu w tym opisu struktur zbiorów i ich zależności;

c) nadzorowanie przestrzegania przez wszystkich użytkowników stosowania obowiązujących procedur;

d) weryfikowanie listy autoryzowanych użytkowników systemów informatycznych;

e) doradzanie użytkownikom w zakresie bezpieczeństwa;

f) zapewnienie, aby cały personel posiadający dostęp do systemu posiadał stosowne zezwolenia oraz był przeszkolony w zakresie obowiązujących regulacji bezpieczeństwa;

g) przygotowanie i prowadzenie „Ewidencji osób biorących udział w przetwarzaniu danych osobowych”;

h) prowadzenie kontroli w zakresie bezpieczeństwa;

i) przygotowywanie wniosków pokontrolnych.

C. UŻYTKOWNIK SYSTEMU

Użytkownik systemu wykonuje wszystkie prace niezbędne do efektywnej oraz bezpiecznej pracy na stanowisku pracy również z wykorzystaniem stacji roboczej. Jest odpowiedzialny przed Administratorem Bezpieczeństwa Informacji za nadzór, implementację i utrzymanie niezbędnych warunków bezpieczeństwa w szczególności do przestrzegania procedur dostępu do systemu i ochrony danych osobowych.

D. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

1. Bezpieczeństwo w przetwarzaniu danych osobowych w formie tradycyjnej.

   Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych pozostają zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia, w których znajdują się zbiory danych osobowych musi być poprzedzone przeniesieniem zbioru danych do odpowiednio zabezpieczonego miejsca. Przy planowanej dłuższej nieobecności pracownika pomieszczenie winno być zamknięte na klucz.

   Klucze do szaf, w których przechowywane są dane osobowe mają jedynie pracownicy upoważnieni do przetwarzania danych osobowych w zakresie zgodnym z kategorią danych. Dostęp do pokoi jest kontrolowany za pomocą monitoringu wizyjnego.

   Korzystanie ze zbiorów danych osobowych przez osoby niezatrudnione w Jednostce powinno odbywać się po uzyskaniu upoważnienia lub skonsultowane z ABI w przypadku osób upoważnionych do przetwarzania tych danych na podstawie ogólnie obowiązujących przepisów.

2. Bezpieczeństwo w przetwarzaniu danych osobowych w systemach informatycznych.

   Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w *Instrukcji Zarządzania Systemem Informatycznym,* obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego szkoły.

III. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Dane osobowe są gromadzone, przechowywane i przetwarzane w kartotekach, skorowidzach, księgach, wykazach oraz w innych zbiorach ewidencyjnych poszczególnych komórek organizacyjnych Szkoły w postaci dokumentów papierowych.

Do przetwarzania zbiorów danych osobowych w systemie informatycznym Szkoły, stosowane są pakiety biurowe lub specjalizowane aplikacje (programy).

Zestawieniazbiorów danych oraz programów stanowiązałączniki nr 5 i 6 do niniejszego regulaminu.

IV. SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

Obieg dokumentów zawierających dane osobowe, pomiędzy komórkamiorganizacyjnymi Szkoły, winien odbywać w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji).

Przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną Szkoły, w miarę możliwości, powinno odbywać się w sposób szyfrowany.

V. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

Dostęp do danych wprowadzonych przez użytkowników systemów informatycznych mają jedynie Administrator Danych Osobowych, upoważnieni pracownicy oraz Administrator Bezpieczeństwa Informacji zapewniający jego prawidłową eksploatację. Wszyscy pracownicy, będący użytkownikami systemu zobowiązani są do zachowania tych danych w tajemnicy.

Ochronie podlegają dane osobowe gromadzone i przetwarzane w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych oraz w urządzeniach i systemie informatycznym Szkoły.

Pomieszczenia, w których przetwarza się dane osobowe powinny być fizycznie zabezpieczone przed dostępem osób nieuprawnionych, to znaczy posiadać odpowiednie zamki do drzwi, zabezpieczenia w oknach (w szczególności na parterze) oraz być wyposażone w środki ochrony ppoż. (gaśnice).

Dokumenty i nośniki informacji, zawierające dane osobowe powinny być zabezpieczone przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane powinny być przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia.

Zasady zabezpieczania danych:

a) zbiory kartotekowe winny znajdować się w zamkniętych pomieszczeniach zabezpieczonych przed dostępem osób nieupoważnionych;

b) zbiory w systemach informatycznych winny być zabezpieczone hasłem dostępu znanym użytkownikowi zbioru.

VI. UDOSTĘPNIANIE POSIADANYCH W ZBIORZE DANYCH OSOBOWYCH

1. Do udostępniania posiadanych w zbiorze danych osobowych upoważniony jest Administrator Danych Osobowych lub pracownik posiadający wymagane prawem upoważnienie.
2. W przypadku udostępniania danych osobowych w celach innych niż włączenie do zbioru, Administrator Danych Osobowych udostępnia posiadane w zbiorze dane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

VII. BEZPIECZEŃSTWO PERSONELU

A. INFORMACJE OGÓLNE

Należy mieć świadomość, że każdy, kto ma dostęp do pomieszczenia, w którym zainstalowano sprzęt systemu informatycznego może spowodować jego uszkodzenie lub może mieć dostęp do informacji wyświetlanych na monitorze lub wydruków.

Zagrożenia w stosunku do systemu mogą pochodzić również od każdej innej osoby np. personelu pomocniczego, technicznego, konsultanta itp., posiadającej wystarczające umiejętności i wiedzę, aby uzyskać dostęp do sieci.

B. UŻYTKOWNICY SYSTEMU

Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa.

Hasło podlega szczególnej ochronie. Użytkownik ma obowiązek tworzenia haseł o długości min. 8 znaków, nie trywialnych lub słownikowych, tzn. nie może używać imion, danych identyfikujących użytkownika oraz jego najbliższych, oraz nie może tworzyć haseł przez kombinację tych nazw lub ich zmianę uporządkowania np. od tyłu. Jest wprowadzony wymóg zabraniający dokonywana zapisów haseł przez użytkowników. W przypadku, gdy użytkownik zapomni swoje hasło, może on uzyskać nowe hasło od Administratora Bezpieczeństwa Informacji zgodnie z obowiązująca procedurą.

VIII. BEZPIECZEŃSTWO FIZYCZNE

A. INFORMACJE OGÓLNE

Informacja przetwarzana i przechowywana w systemie musi być zabezpieczona w szczególny sposób.

Środki bezpieczeństwa fizycznego są konieczne dla zapobiegania niepowołanemu dostępowi do informacji, nieautoryzowanym operacjom w systemie, kontroli dostępu do zasobów oraz w celu zabezpieczenia sprzętu teleinformatycznego.

B. POMIESZCZENIA LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE - OBSZAR SYSTEMU

Obszarem do przetwarzania danych osobowych z użyciem sprzętu komputerowego są:

a) sekretariat,
b) gabinet dyrektora,
c) gabinet wicedyrektora,
d) pokój nauczycielski,
e) pokój kadr i kierownika administracyjno-gospodarczego,
f) pokój księgowości,
g) biblioteka szkolna,
h) gabinet pedagoga i psychologa szkolnego,
i) wszystkie sale lekcyjne wyposażone na stanowiskach nauczycielskich w komputery

Pomieszczenia te zabezpieczone są w następujący sposób: zamki, szkolny monitoring.

C. OCHRONA SERWERA, STACJI ROBOCZYCH I NOŚNIKÓW

Pomieszczenia, w których znajdują się stanowiska komputerowe są:

a) zamknięte, jeśli nikt w nich nie przebywa;
b) wyposażone w zamykane szafy umożliwiające przechowywanie dokumentów.

Szkolny serwer znajduje się w zamkniętym pomieszczeniu, do którego dostęp ma tylko ADO i ABI oraz opiekun pracowni.

D. ZASADY KONTROLI SPRZĘTU

Instalacja urządzeń systemu i sieci teleinformatycznej odbywa się za wiedzą i pod kontrolą Administratora Danych Osobowych, który jest również odpowiedzialny za warunki wprowadzania do użycia, przechowywania, eksploatacji oraz wycofywania z użycia każdego urządzenia.

IX. BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

A. INFORMACJE OGÓLNE

Sprzęt i oprogramowanie, indywidualnie lub łącznie mają ścisły związek z bezpieczeństwem systemu i sieci teleinformatycznej. Dlatego, powinny być ściśle przestrzegane procedury bezpieczeństwa odnoszące się do tych elementów.

B. BEZPIECZEŃSTWO SPRZĘTOWE

Sieć teleinformatyczna jest organizacyjnym i technicznym połączeniem systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi. Niedopuszczalne jest samowolne przemieszczanie lub zmiana konfiguracji stacji roboczej bez wiedzy Administratora Bezpieczeństwa Informacji.

C. BEZPIECZEŃSTWO OPROGRAMOWANIA

Nie zezwala się na korzystanie z jakiegokolwiek nowego oprogramowania bez zgody Administratora Bezpieczeństwa Informacji. Dodatkowe oprogramowanie może być instalowane wyłącznie przez Administratora Bezpieczeństwa Informacji. Kopieoprogramowania operacyjnego, aplikacyjnego i użytkowego przechowuje się częściowo w pokoju kierownika administracyjno-gospodarczego, częściowo w zabezpieczonym pomieszczeniu na zapleczu sali nr 1, częściowo w pracowni komputerowej nr 107.

Używanie oprogramowania prywatnego w sieci jest kategorycznie zabronione. Na stacjach roboczych powinno być zainstalowane jedynie niezbędne oprogramowanie.

X. KONSERWACJE I NAPRAWY

A. KONSERWACJA SPRZĘTU

Każde urządzenie użytkowane w systemie informatycznym, powinno podlegać rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby.

B. KONSERWACJA OPROGRAMOWANIA

Za konserwację oprogramowania systemowego oraz aplikacyjnego serwera systemu informatycznego odpowiedzialny jest Administrator Bezpieczeństwa Informacji. Konserwacja ww. oprogramowania obejmuje także jego aktualizację.

Za konserwację oprogramowania stanowisk roboczych odpowiedzialny jest Administrator Danych Osobowych. Wszelkie aktualizacje oprogramowania powinny być uzgadniane z Administratorem Bezpieczeństwa Informacji.

C. NAPRAWA SPRZĘTU

Administrator Bezpieczeństwa Informacji przed rozpoczęciem naprawy urządzenia przez zewnętrzne firmy sprawdza, czy spełnione są następujące wymagania:

a) w przypadku awarii serwera i konieczności oddania sprzętu do serwisu, nośniki magnetyczne zawierające dane osobowe powinny być wymontowane i do czasu naprawy serwera przechowywane w szafie metalowej znajdującej się w strefie o ograniczonym dostępie;

b) w przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia.

XI. PLANY AWARYJNE I ZAPOBIEGAWCZE

A. ZASILANIE

Serwer systemu oraz poszczególne stacje robocze (opcjonalnie) powinny być zabezpieczone urządzeniami podtrzymującymi zasilanie (UPS), co umożliwi funkcjonowanie systemu w przypadku awarii zasilania.

B. KOPIE ZAPASOWE

W celu zabezpieczenia ciągłości pracy, informacja przechowywana i przetwarzana w systemie podlega codziennej, przyrostowej archiwizacji (opcjonalnie) oraz pełnej archiwizacji przeprowadzanej nie rzadziej niż raz na miesiąc. Kopie archiwalne danych są wykonywane na nośnikach magnetooptycznych, i przechowywane są przez Administratora Bezpieczeństwa Informacji. Użycie kopii zapasowych następuje na polecenie Administratora Bezpieczeństwa Informacji w przypadku odtwarzania systemu po awarii.

XII. POLITYKA ANTYWIRUSOWA

W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:

a) nie należy używać oprogramowania na stacji roboczej innego niż zaleca Administrator Bezpieczeństwa Informacji

b) nie wolno instalować oprogramowania typu freeware czy shareware;

c) regularnie uaktualniać bazę wirusów zainstalowanego oprogramowania antywirusowego;

d) przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.

XIII. UDOSTĘPNIANIE DANYCH OSOBOWYCH

Każda osoba, której dane osobowe są przetwarzane w systemie informatycznym, ma prawo uzyskać na piśmie, w powszechnie zrozumiałej formie, treść tych danych oraz następujące informacje:

a) datę pierwszego wprowadzenia danych tej osoby,

b) źródło pochodzenia danych,

c) identyfikator użytkownika wprowadzającego dane,

d) jakim uprawnionym podmiotom, kiedy i w jakim zakresie dane zostały udostępnione.

XIV. POSTANOWIENIA KOŃCOWE

W sprawach nieobjętych niniejszym regulaminem maja zastosowanie przepisy ustawy o ochronie danych osobowych.

Regulamin wchodzi w życie z dniem ogłoszenia.