ZARZĄDZENIE NR 10/2017
DYREKTORA CENTRUM USŁUG WSPÓLNYCH W NOWEJ SARZYNIE
z dnia 31 maja 2017 r.

w sprawie wprowadzenia „Polityki bezpieczeństwa danych osobowych przetwarzanych w Centrum Usług Wspólnych w Nowej Sarzynie" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Usług Wspólnych w Nowej Sarzynie"

Na postawie art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz.922) oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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. Nr 100, poz. 1024), **zarządzam:**

§ 1

Wprowadzić do stosowania „Politykę bezpieczeństwa danych osobowych przetwarzanych w Centrum Usług Wspólnych w Nowej Sarzynie", stanowiącą Załącznik nr 1 do niniejszego zarządzenia.

§ 2

Wprowadzić do stosowania „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Usług Wspólnych w Nowej Sarzynie", stanowiącą Załącznik nr 2 do niniejszego zarządzenia.

§ 3

Nadzór nad realizacją zarządzenia powierza się Dyrektorowi Centrum Usług Wspólnych w Nowej Sarzynie.

§ 4

Traci moc Zarządzenie Nr 3/2016 Dyrektora Zespołu Ekonomiczno-Administracyjnego Szkół i Przedszkoli w Nowej Sarzynie z dnia 12 grudnia 2016 r. w sprawie wprowadzenia „Polityki bezpieczeństwa danych osobowych przetwarzanych w Zespole Ekonomiczno-Administracyjnym Szkół i Przedszkoli w Nowej Sarzynie" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Ekonomiczno-Administracyjnym Szkół i Przedszkoli w Nowej Sarzynie".

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Centrum Usług Wspólnych w Nowej Sarzynie
Józef Dziurdź

Załącznik nr 1
do Zarządzenia Nr 10/2017
Dyrektora Centrum Usług Wspólnych
w Nowej Sarzynie
z dnia 31 maja 2017 r.

Zatwierdzam:

Dziurdź Józef
ADO

DYREKTOR
Centrum Usług Wspólnych w Nowej Sarzynie
Józef Dziurdź

Wysocka Iwona
ABI

Polityka Bezpieczeństwa Danych Osobowych Przetwarzanych w Centrum Usług Wspólnych w Nowej Sarzynie

Nowa Sarzyna 2017

SPIS TREŚCI

1. Postanowienia ogólne

1.1. Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

1) CUW – należy przez to rozumieć Centrum Usług Wspólnych w Nowej Sarzynie,
2) Administratorze Danych Osobowych (ADO) – należy przez to rozumieć Dyrektora Centrum Usług Wspólnych w Nowej Sarzynie,
3) Administratorze Bezpieczeństwa Informacji (ABI) – należy przez to rozumieć osobę powołaną do nadzorowania przestrzegania zasad ochrony danych osobowych określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony danych osobowych wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych,
4) Administratorze Systemu Informatycznego (ASI) – należy przez to rozumieć osobę zajmującą stanowisko informatyka,
5) użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym CUW. Użytkownikiem może być pracownik CUW, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w CUW,
6) systemie informatycznym – jest to zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej w CUW.

1.2. Cel

Celem Polityki bezpieczeństwa danych osobowych przetwarzanych w CUW w Nowej Sarzynie, zwanej dalej Polityką bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania grupy informacji zawierającej dane osobowe.

Polityka bezpieczeństwa została opracowana w związku z wymaganiami zawartymi w:

- ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2016 r. poz. 922) 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).

Politykę bezpieczeństwa opracowano poprzez:

- wskazanie pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
- wskazanie wykazu zbiorów danych osobowych przetwarzanych w ramach systemu informatycznego,
- opis struktury zbiorów danych wraz z ich merytoryczna zawartością,
- wskazanie sposobu przepływu danych pomiędzy systemem informatycznym i innymi systemami informatycznymi,
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych w CUW,
- określenie administracji i organizacji bezpieczeństwa przetwarzanych danych w CUW,
- określenie zasad bezpieczeństwa osobowego,
- określenie zasad bezpieczeństwa fizycznego,
- określenie zasad bezpieczeństwa sprzętu i oprogramowania,
- określenie zasad konserwacji i napraw sprzętu funkcjonującego w systemie informatycznym,
- określenie planów awaryjnych i zapobiegawczych,
- określenie polityki antywirusowej.

Opracowanie polityki bezpieczeństwa dla CUW służy ochronie przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

1.3. Zakres stosowania

1. Niniejsza polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w CUW w systemie informatycznym oraz prowadzonych w tym zakresie zbiorów w formie tradycyjnej.
2. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób

upoważnionych do przetwarzania danych osobowych w CUW, zarówno zatrudnionych (np. umowa o pracę, umowa zlecenia, umowa o dzieło), jak i świadczących pracę na rzecz CUW (np. stażystów, praktykantów).

3. Do zapoznania się z niniejszym dokumentem oraz stosowania zawartych w nim zasad zobowiązani są wszyscy pracownicy CUW oraz osoby określone w ust. 2 upoważnieni do przetwarzania danych osobowych.

4. Wszystkie osoby, których rodzaj wykonywanej pracy wiąże się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w CUW zasad ochrony danych osobowych.

1.4. Poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym

Uwzględniając kategorie przetwarzanych danych osobowych oraz zagrożenia wprowadza się wysoki poziom bezpieczeństwa w systemie informatycznym służącym do przetwarzania danych osobowych.

2. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Dane osobowe przetwarzane są w budynku Urzędu Miasta i Gminy Nowa Sarzyna, w którym zlokalizowany jest na pierwszym piętrze Centrum Usług Wspólnych w Nowej Sarzynie, przy ulicy Mikołaja Kopernika 1.

Pomieszczenia, w których wykonuje się operacje na danych osobowych w ramach systemu (przegląda, wprowadza, zmienia, kasuje):

CUW, piętro 1	pok. nr 1
CUW, piętro 1	pok. nr 2
CUW, piętro 1	pok. nr 3
CUW, piętro 1	pok. nr 4
CUW, piętro 1	pok. nr 5
CUW, piętro 1	pok. nr 6
CUW, piętro 1	pok. nr 7
CUW, piętro 1	pok. nr 8
CUW, piętro 1	pok. nr 9
CUW, piętro 1	pok. nr 10

3. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Lp.	Nazwa zbioru	Sposób gromadzenia	Program służący do przetwarzania danych
1.	Akta osobowe pracowników	Forma papierowa i elektroniczna	Kadry Optivum firmy VULCAN
2.	Arkusze organizacyjne szkół	Forma papierowa i elektroniczna	Sigma firmy VULCAN
3.	Sprawozdawczość SIO	Forma papierowa i elektroniczna	SIO program Ministerstwa Edukacji Narodowej
4.	Dofinansowanie kosztów kształcenia pracowników młodocianych	Forma papierowa	-
5.	Konkursy na stanowiska w jednostkach oświatowych	Forma papierowa	-
6.	Opiniowanie i zatrudnianie osób zatrudnionych w jednostkach	Forma papierowa	-
7.	Programy pomocy materialnej dla uczniów	Forma papierowa	-
8.	Dowóz uczniów do szkół	Forma papierowa	-
9.	Umowy z kontrahentami	Forma papierowa	-
10.	Dane płacowe	Forma papierowa elektroniczna	Płace Optivum firmy VULCAN Płatnik firmy Asseco Poland
11.	Ewidencja korespondencji i adresów e-mail	Forma papierowa	-

4. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

4.1 Kadry Optivum firmy VULCAN

Opis struktury zbiorów danych

Baza danych w formacie .mdf (MS SQL) umieszczona na serwerze.

Zawartość merytoryczna

Imię i nazwisko, nazwisko rodowe, imiona rodziców, data i miejsce urodzenia, obywatelstwo, PESEL,NIP, nr i seria dowodu osobistego, miejsce zameldowania (dokładny adres), adres do korespondencji, telefon, wykształcenie przebieg dotychczasowego zatrudnienia, rodzina, kwalifikacje, powszechny obowiązek wojskowy (stosunek do powszechnego obowiązku obrony, stopień wojskowy numer specjalności wojskowej, przynależność ewidencyjna do WKU, numer książeczki wojskowej, przydział mobilizacyjny do sił zbrojnych RP) osoba, którą

należy zawiadomić w razie wypadku, umowa o pracę, rodzaj wykonywanej pracy (stanowisko, funkcja zawód, specjalność), miejsce zatrudnienia, wynagrodzenie, wysługa lat, dodatkowe dane do kontaktu, badania lekarskie.

4.2 Sigma firmy VULCAN

Opis struktury zbiorów danych

Baza danych umieszczona na zewnętrznym serwerze firmy VULCAN.

Zawartość merytoryczna

Zbiór danych o pracownikach pedagogicznych oraz zbiorczy arkusz organizacyjny jednostek oświatowych z terenu Miasta i Gminy Nowa Sarzyna.

4.3 Płace Optivum firmy VULCAN

Opis struktury zbiorów danych

Baza danych w formacie .mdf (MS SQL) umieszczona na serwerze.

Zawartość merytoryczna

Imię, nazwisko, PESEL, NIP, adres zamieszkania, data urodzenia, imię ojca, imię matki, miejsce urodzenia, obywatelstwo, numer i seria dowodu osobistego, przez kogo dowód osobisty wystawiony, Urząd Skarbowy, wynagrodzenie zasadnicze, dodatki – specjalny, stażowy, funkcyjny; premia, składka na ubezpieczenia: zdrowotne, społeczne, wypadkowe, chorobowe, zdrowotne: podatek, składka na ubezpieczenie dobrowolne (PZU), wkłady na kasę zapomogowo - pożyczkową, potrącenia od płacy, okresy zatrudnienia, kod tytułu ubezpieczeniowego, nr konta bankowego.

4.4 Płatnik firmy Asseco Poland

Opis struktury zbiorów danych

Baza danych w formacie .mdb (MS Access) umieszczona na lokalnej stacji roboczej.

Zawartość merytoryczna

Numer identyfikacji podatkowej NIP, numer ewidencyjny PESEL, rodzaj dokumentu tożsamości, seria i numer dokumentu tożsamości, nazwisko, imię data urodzenia, imię drugie, nazwisko rodowe, obywatelstwo, płeć czy cudzoziemiec posiada kartę stałego pobytu, czy cudzoziemiec posiada kartę czasowego pobytu, niezdolności do pracy, kod wykonywanego zawodu, kod stanowiska, kod wykształcenia, kod pracy w szczególnych warunkach, nazwa kasy chorych, data zawarcia umowy z kasą chorych, kod pocztowy, miejscowość, gmina, ulica,

numer domu, numer lokalu, numer telefonu, numer identyfikacji podatkowej NIP członka rodziny, numer ewidencyjny PESEL członka rodziny, rodzaj dokumentu tożsamości członka rodziny, seria i numer dokumentu tożsamości członka rodziny, nazwisko członka rodziny, imię członka rodziny, data urodzenia członka rodziny, stopień pokrewieństwa członka rodziny.

4.5 SIO program Ministerstwa Edukacji Narodowej

Opis struktury zbiorów danych

Baza danych w formacie . sqlite umieszczona na lokalnej stacji roboczej.

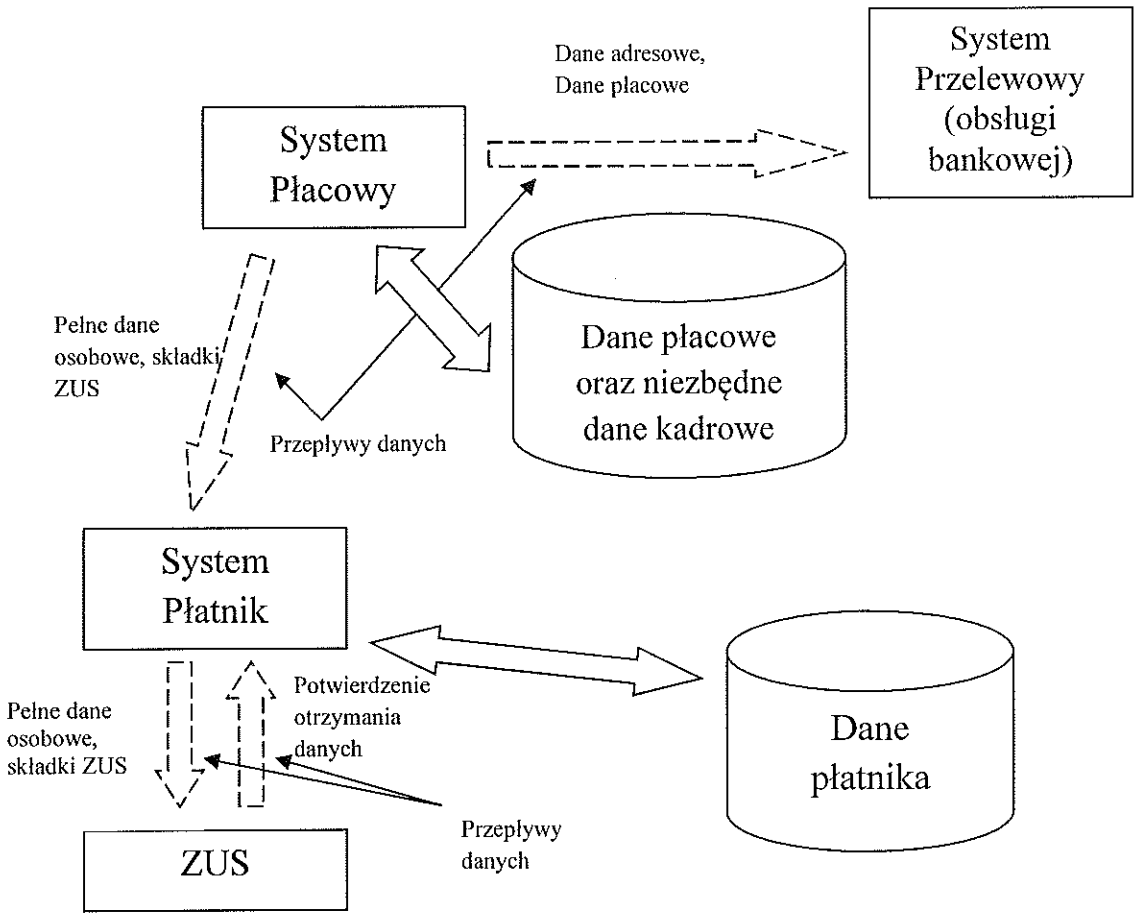
Zawartość merytoryczna

Wykorzystuje wygenerowane dane z jednostek oświatowych z terenu Miasta i Gminy Nowa Sarzyna, szyfruje i pakuje dane tworząc plik z rozszerzeniem .exp – plik przesyłany jest do Kuratorium Oświaty w Rzeszowie.

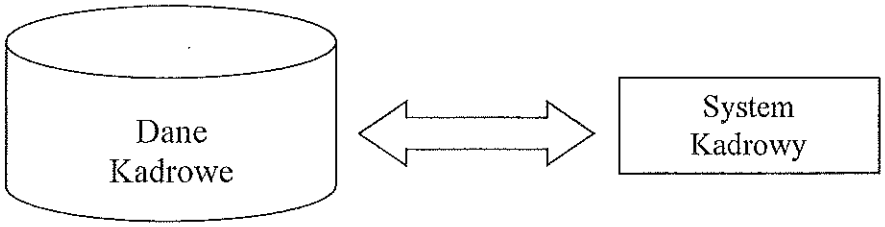
PESEL, płeć, wykształcenie, nazwa szkoły i rok ukończenia, warunki zatrudnienia, staż pracy, historia pracy, kary, nagrody, tytuł zawodowy, zawód wyuczony i wykonywany, uzyskane kwalifikacje, nieobecności w pracy.

5. Sposób przepływu danych pomiędzy poszczególnymi systemami

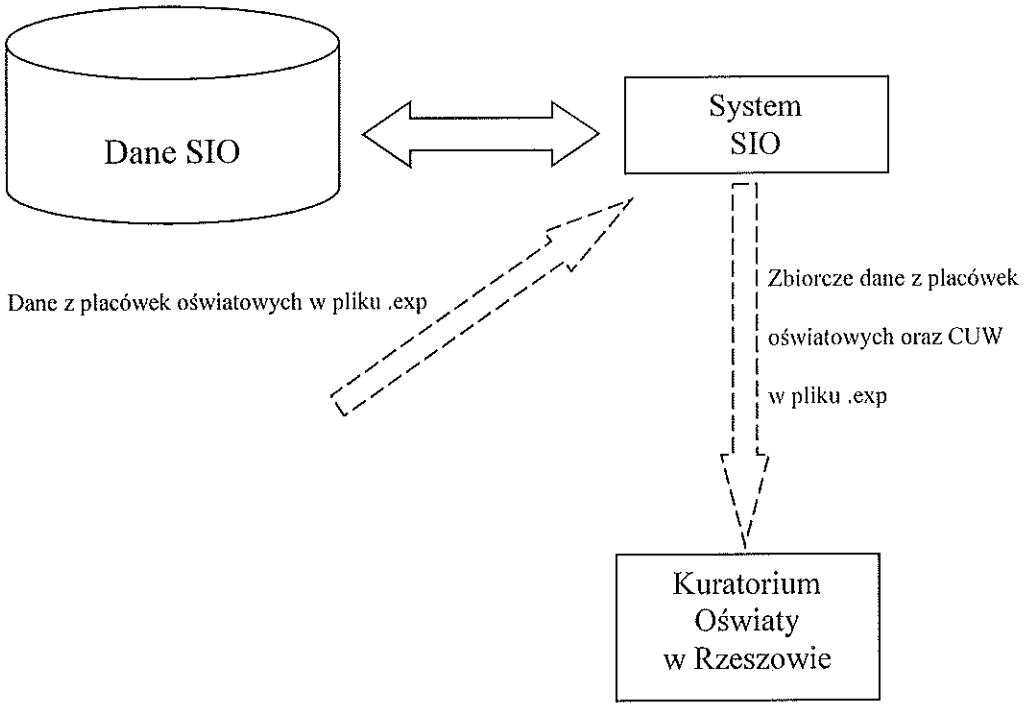
5.1 System płacowy



5.2 System kadrowy



5.3 SIO program Ministerstwa Edukacji Narodowej



6. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności przetwarzanych danych.

Bezpieczeństwo danych osobowych przetwarzanych w CUW jest związane z zachowaniem ich trzech podstawowych atrybutów:

- **poufności**, czyli zagwarantowaniem, że dane osobowe nie są udostępniane lub ujawniane nieuprawnionym osobom, podmiotom lub procesom,
- **integralności**, czyli zapewnieniem, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- **rozliczalności**, czyli zapewnieniem, że operacje wykonywane na danych osobowych są przypisane w sposób jednoznaczny umożliwiający identyfikację osoby która te operacje wykonywała.

6.1. Zapewnienie poufności przetwarzanych danych

W zakresie zapewnienia poufności przetwarzanych danych:

- użytkownicy przetwarzający dane osobowe w CUW są szkoleni w zakresie ochrony danych osobowych,
- osoby zatrudnione przy przetwarzaniu danych w CUW zostały zobowiązane do zachowania w tajemnicy tych danych oraz szczegółów technicznych zabezpieczeń, metod i sposobów pracy, także po ustaniu zatrudnienia,
- prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych w CUW,
- użytkownicy przetwarzający dane osobowe w systemie informatycznym posiadają własne identyfikatory i hasła dostępu,
- niezwłocznie po ustaniu zatrudnienia, zawieszeniu w czynnościach służbowych użytkownicy są pozbawiani praw dostępu do systemu informatycznego,

- hasła są zbudowane wg zasad określonych dla wysokiego poziomu bezpieczeństwa, zawierają małe i wielkie litery oraz cyfry lub znaki specjalne oraz, zgodnie z zaleceniami, są zmieniane raz na miesiąc.

6.2. Zapewnienie integralności przetwarzanych danych

W zakresie zapewnienia integralności przetwarzanych danych:

- kopie zapasowe zbiorów danych przechowywane są w serwerowni,
- oprogramowanie antywirusowe jest na bieżąco aktualizowane,
- dokumenty w formie papierowej, będące roboczymi raportami, zawierające dane osobowe, których okres przydatności się skończył są niszczone w sposób mechaniczny za pomocą niszczarek,
- elektroniczne nośniki danych są niszczone komisyjnie (dotyczy to w szczególności płyt CD/DVD zawierających kopie awaryjne), niszczenie odbywa się w sposób uniemożliwiający odczyt zapisanych na nośnikach danych.

6.3. Rozliczalność przetwarzanych danych

W zakresie rozliczalności przetwarzanych danych:

- każdy użytkownik systemu informatycznego posiada odrębny identyfikator,
- posiadanie imiennych upoważnień i indywidualnych zakresów czynności wydanych przez ADO,
- system informatyczny jest wyposażony w mechanizmy pozwalające w sposób jednoznaczny przypisać wykonanie określonych operacji na danych osobowych konkretnemu użytkownikowi.

7. Zasady, normy i wymagania zgodności mające szczególne znaczenie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych.

7.1. Zabezpieczenie techniczne

1. Szczegółowy opis zabezpieczenia pomieszczeń i obiektu zawiera „Instrukcja postępowania z kluczami oraz zabezpieczenia pomieszczeń i obiektu Centrum Usług Wspólnych w Nowej Sarzynie".
2. Dane przetwarzane przy użyciu tradycyjnych środków pisarskich gromadzone są w rejestrach, księgach, zeszytach papierowych oraz segregatorach i przechowywane w zamykanych szafach oraz kasach pancernych.
3. Pomieszczenie w którym przechowywane są kopie zapasowe z CUW posiada alarm przeciwpożarowy.
4. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
5. Do ochrony sieci wewnętrznej CUW wykorzystywane jest urządzenie Firewall z funkcjonalnością UTM (zintegrowane zarządzanie zagrożeniami) oferujące ochronę antyspamową, antywirusową, wykrywanie intruzów, zapobieganie wtargnięciu intruzów, filtrowanie treści internetowych oraz posiadające funkcje zapory ogniowej.
6. Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

7.2. Bezpieczeństwo osobowe

1. Dostęp do danych wprowadzonych przez użytkowników systemu informatycznego mają jedynie upoważnieni pracownicy oraz Informatyk zapewniający jego prawidłową eksploatację.
2. Wszyscy pracownicy, będący użytkownikami systemu informatycznego zobowiązani są do zachowania tych danych w tajemnicy.
3. Wszyscy użytkownicy systemu informatycznego muszą stosować się do obowiązujących procedur bezpieczeństwa.
4. Wszyscy użytkownicy systemu informatycznego korzystają z informacji przechowywanej i przetwarzanej w systemie informatycznym na zasadach wiedzy

koniecznej, po uprzednim potwierdzeniu znajomości zasad wynikających z procedur bezpieczeństwa.

5. W pomieszczeniach, w których przetwarzane są dane osobowe i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.
6. Należy mieć świadomość, że każdy, kto ma dostęp do pomieszczeń, w których zainstalowano sprzęt systemu informatycznego służącego do przetwarzania danych osobowych może spowodować jego uszkodzenie lub może mieć dostęp do informacji wyświetlanych na monitorze lub wydruków.
7. Lista wszystkich użytkowników systemu informatycznego funkcjonującego w CUW znajduje się u Informatyka.

7.3. Konserwacje i naprawy

1. Przeprowadza się przeglądy całości sprzętu komputerowego i posiadanych licencji oprogramowania (minimum raz w roku lub w razie konieczności) w zakresie:
   - sprawdzenia zainstalowanego oprogramowania (sprawdzenie legalności),
   - sprawdzenia stanu technicznego zestawu komputerowego i urządzeń peryferyjnych,
   - określenia zapotrzebowania w zakresie sprzętu i oprogramowania,
   - sprawdzenia stabilności i czyszczenia systemu operacyjnego.
2. Każde urządzenie użytkowane w systemie informatycznym wykorzystywanym do przetwarzania danych osobowych, podlega rutynowym czynnościom konserwacyjnym oraz przeglądom wykonywanym przez uprawnione osoby.
3. Za konserwację oprogramowania systemowego, aplikacyjnego odpowiada ASI. Konserwacja ww. oprogramowania obejmuje także jego aktualizację.
4. Za konserwację i utrzymanie serwera systemu informatycznego oraz stanowisk roboczych odpowiedzialny jest ASI.
5. W przypadku naprawy urządzenia przez zewnętrzne firmy ASI zobowiązany jest, przed rozpoczęciem naprawy, zapewnić, aby:
   - pracownicy techniczni firmy zewnętrznej dokonywali naprawy serwera w wyznaczonym pomieszczeniu pod nadzorem ASI,

- w przypadku awarii serwera i konieczności oddania sprzętu do serwisu, nośniki magnetyczne zawierające dane osobowe zostały wymontowane i do czasu naprawy serwera przechowywane w zamkniętej szafie znajdującej się w strefie o ograniczonym dostępie.

6. W przypadku uszkodzenia nośnika magnetycznego zawierającego dane osobowe należy komisyjnie dokonać jego zniszczenia.

7.4. Polityka antywirusowa

1. W zakresie ochrony antywirusowej wprowadza się następujące zalecenia:
   - należy regularnie uaktualniać bazę wirusów zainstalowanego oprogramowania antywirusowego,
   - przed użyciem nośnika danych sprawdzić czy nie jest zainfekowany wirusem komputerowym.
2. Wszystkie stacje robocze mają zainstalowane oprogramowanie antywirusowe, które jest uaktywniane podczas uruchamiania stacji roboczej.

Załącznik nr 2
do Zarządzenia Nr 10/2017
Centrum Usług Wspólnych w Nowej
Sarzynie z dnia 31 maja 2017 r .

Zatwierdzam:

Dziurdź Józef
DYREKTOR
Centrum Usług Wspólnych w Nowej Sarzynie
ADO
Józef Dziurdź

Wysocka Iwona
ABI

INSTRUKCJA ZARZĄDZANIA

SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM

DO PRZETWARZANIA DANYCH OSOBOWYCH

W CENTRUM USŁUG WSPÓLNYCH W NOWEJ SARZYNIE

Nowa Sarzyna 2017

SPIS TREŚCI

1. Postanowienia ogólne

1.1 Podstawa prawna

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2016r. poz. 922) oraz rozporządzenie 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. Nr 100, poz. 1024) nakładają na administratora danych osobowych następujące obowiązki:

- zapewnienie bezpieczeństwa i poufności danych, w tym zabezpieczenie ich przed ujawnieniem,
- zabezpieczenie danych przed nieuprawnionym dostępem,
- zabezpieczenie danych przed udostępnieniem osobom nieupoważnionym (nieuprawnionym pozyskaniem),
- zabezpieczenie przed utratą danych,
- zabezpieczenie przed uszkodzeniem lub zniszczeniem danych oraz przed ich nielegalną modyfikacją.

1.2 Definicje

Ilekroć w niniejszym dokumencie jest mowa o:

1) CUW – należy przez to rozumieć Centrum Usług Wspólnych w Nowej Sarzynie,
2) Administratorze Danych Osobowych (ADO) – należy przez to rozumieć Dyrektora Centrum Usług Wspólnych w Nowej Sarzynie,
3) Administratorze Bezpieczeństwa Informacji (ABI) – należy przez to rozumieć pracownika CUW lub inną osobę powołaną do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych,
4) Administratorze Systemu Informatycznego (ASI) - należy przez to rozumieć pracownika CUW zatrudnionego na stanowisku informatyka,
5) użytkowniku systemu – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym CUW. Użytkownikiem może być pracownik CUW, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w CUW,

6) systemie informatycznym – jest to zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej w CUW.

1.3 Cel

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Usług Wspólnych w Nowej Sarzynie, zwana dalej „Instrukcją" jest wewnętrznym dokumentem CUW i określa sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w zbiorach danych.

2. Instrukcja odnosi się do organizacji, metod i trybu przetwarzania danych osobowych oraz konserwacji systemu informatycznego oraz użytych w tym celu środków organizacyjnych i technicznych, ustanawianych przez Administratora Danych Osobowych, a także określa tryb dopuszczania do zasobów systemu informatycznego użytkowników oraz specjalistów z zakresu konserwacji sprzętu i oprogramowania.

3. Instrukcja ma zapewnić zabezpieczenie zasobów technicznych systemu informatycznego, ochronę oprogramowania i danych osobowych przed nieuprawnionymi działaniami (wgląd, modyfikacja, pozyskanie i dalsze ujawnienie), a także przed ich utratą.

4. Instrukcja przeznaczona jest dla pracowników CUW upoważnionych do przetwarzania danych osobowych przez Administratora Danych Osobowych.

2. Osoby odpowiedzialne za funkcjonowanie systemu informatycznego służącego do przetwarzania danych w CUW oraz jego użytkownicy

2.1 Administrator Danych Osobowych (ADO)

Za bezpieczeństwo danych osobowych przetwarzanych w CUW odpowiedzialny jest Administrator Danych Osobowych.

Administrator Danych Osobowych obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

ADO przetwarza dane osobowe zgodnie z prawem oraz realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

- podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem zmian w obowiązującym prawie, organizacji CUW oraz technik zabezpieczenia danych osobowych,
- nadaje upoważnienia do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi czynności,
- wyznacza Administratora Bezpieczeństwa Informacji oraz określa jego zakres czynności,
- udostępnia dane osobowe ze zbioru na żądanie uprawnionych podmiotów w przypadkach wskazanych prawem.

2.2 Administrator Bezpieczeństwa Informacji (ABI)

ABI powołany przez ADO, odpowiada za:

- prowadzenie w imieniu i z upoważnienia ADO, ewidencji osób upoważnionych do przetwarzania danych osobowych,
- przygotowywanie upoważnień do przetwarzania danych osobowych,
- wdrażanie stosownych środków administracyjnych, i technicznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,

- podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie informatycznym, zabezpieczeń w zakresie zbiorów danych osobowych,
- prowadzenie jawnego rejestru danych osobowych przetwarzanych w CUW,
- szkolenie osób dopuszczonych do przetwarzania danych osobowych lub przebywania w obszarze przetwarzania danych osobowych z zakresu zasad przetwarzania i ochrony tych danych oraz zasad bezpieczeństwa informatycznego w oparciu o przygotowywane przez siebie materiały szkoleniowe oraz prowadzenie adekwatnej dokumentacji w tym zakresie (np. potwierdzenie przeszkolenia),
- koordynowanie kontroli wewnętrznych z zakresu przestrzegania przepisów o ochronie danych osobowych,
- sporządzanie wykazu obszarów przetwarzania danych osobowych,

2.3 Administrator Systemu Informatycznego (ASI)

Administrator Systemu Informatycznego (ASI) odpowiada za:

- zarządzanie systemem informatycznym, w którym przetwarzane są dane osobowe,
- zarządzanie systemem komunikacji w sieci komputerowej oraz przesyłania danych za pośrednictwem urządzeń teletransmisji,
- funkcjonowanie mechanizmów uwierzytelniania użytkowników w systemie informatycznym służącym do przetwarzania danych osobowych oraz kontroli dostępu do danych osobowych,
- wykonywanie kopii bezpieczeństwa komputerowych zbiorów danych zgodnie z zasadami określonymi w niniejszej instrukcji,
- prowadzi ewidencję wykonanych kopii zapasowych,
- odpowiada za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego CUW. Po odtworzeniu systemu informatycznego ASI odpowiada za przeprowadzenie testów poprawności działania systemu przed jego oddaniem do użytkowania,
- przydzielanie każdemu użytkownikowi indywidualnego identyfikatora oraz hasła do systemu informatycznego oraz dokonywanie ewentualnych modyfikacji uprawnień, a także w porozumieniu z Dyrektorem usuwanie konta użytkownika,

- wykonywanie lub sprawowanie nadzoru nad wykonywaniem: napraw, konserwacji oraz likwidacji urządzeń komputerowych, które mogą zawierać dane osobowe.

2.4 Pracownik ds. Kadr

Pracownik ds. Kadr odpowiada za:

- przechowywanie upoważnień do przetwarzania danych osobowych w aktach osobowych,
- występowanie z wnioskiem do Administratora Danych Osobowych o nadanie upoważnień do przetwarzania danych osobowych, a także o odwołanie upoważnienia do przetwarzania danych osobowych w przypadku rozwiązania lub wygaśnięcia stosunku pracy.

2.5 Kierownik Działu Kadr, Płac i Obsługi Administracyjnej oraz Główny Księgowy

Kierownik Działu Kadr, Płac i Obsługi Administracyjnej oraz Główny Księgowy są odpowiedzialni za:

- występowanie z wnioskiem do Administratora Danych Osobowych o nadanie oraz modyfikację upoważnienia do przetwarzania danych osobowych,
- nadzorowanie przestrzegania zasad przetwarzania i ochrony danych osobowych przyjętych w CUW przez podległy personel w szczególności do prawidłowego zabezpieczania danych osobowych oraz miejsc ich przechowywania w trakcie i po zakończeniu pracy,
- przeciwdziałania dostępowi osób nieuprawnionych do danych osobowych i systemu informatycznego, w którym są przetwarzane,
- współdziałanie z ABI w zakresie przestrzegania zasad przetwarzania i ochrony danych osobowych w CUW oraz identyfikacji i analizy ryzyk z tym związanych,
- niezwłoczne informowanie ABI, o każdym stwierdzeniu lub podejrzeniu naruszenia bezpieczeństwa danych osobowych lub systemu informatycznego, w którym są przetwarzane oraz współdziałanie przy usuwaniu skutków takiego naruszenia.

2.6 Osoby przetwarzające dane osobowe

Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do:

- przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez ADO w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków,
- poznania i bezwzględnego przestrzegania obowiązujących w CUW zasad przetwarzania i ochrony danych osobowych oraz bezpieczeństwa systemu informatycznego,
- zachowania w tajemnicy danych, które przetwarza oraz sposobów ich zabezpieczenia przez cały okres zatrudnienia w CUW, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji,
- korzystania z systemu informatycznego w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników oraz zasadami przyjętymi w CUW,
- zabezpieczania danych osobowych oraz informacji o zabezpieczeniach systemu informatycznego przed ich udostępnianiem osobom nieuprawnionym, nieuprawnioną modyfikacją, utratą lub zniszczeniem.

3. Nadawanie/odbieranie uprawnień do przetwarzania danych w systemie informatycznym

Dane osobowe w systemie informatycznym w CUW może przetwarzać wyłącznie osoba posiadająca aktualne, ważne pisemne upoważnienie do przetwarzania danych osobowych.
W przypadku ustania stosunku pracy/zmiany zakresu obowiązków użytkownika, następuje odebranie użytkownikowi praw dostępu do systemu informatycznego.

TRYB POSTĘPOWANIA

1. Dane osobowe w systemie informatycznym może przetwarzać wyłącznie osoba posiadająca aktualne, ważne pisemne upoważnienie do przetwarzania danych osobowych. Wzór upoważnienia stanowi **Załącznik nr 1** do niniejszego opracowania.
2. Upoważnienie do przetwarzania danych osobowych wydaje ADO.
3. Zarejestrowanie użytkownika w systemie informatycznym i nadanie mu upoważnienia do przetwarzania danych osobowych następuje na wniosek kierownika Działu Kadr, Płac i Obsługi Administracyjnej bądź Głównego Księgowego, którego wzór stanowi **Załącznik nr 2** do niniejszego opracowania.
4. Dla każdej osoby upoważnionej do przetwarzania danych osobowych ABI tworzy indywidualny zakres czynności, którego wzór stanowi **Załącznik nr 3** do niniejszego opracowania.
5. ASI rejestruje użytkownika w systemie i konfiguruje jego konto, nadając mu uprawnienia do pracy w systemie informatycznym na podstawie upoważnienia do przetwarzania danych osobowych wydanego przez ADO.
6. Odebranie uprawnień użytkownika następuje w przypadku zaistnienia okoliczności, warunkujących wyrejestrowanie użytkownika z systemu i blokadę jego konta.
7. Takimi okolicznościami są m.in.:
   - zwolnienie z pracy;
   - zmiana zakresu obowiązków powodująca, że pracownik nie będzie już przetwarzał danych osobowych w systemie informatycznym,
   - nieobecność w pracy trwająca dłużej niż 6 miesięcy.
8. ABI prowadzi rejestr osób upoważnionych do przetwarzaniu danych osobowych wg **Załącznika nr 4** do niniejszego opracowania.

4. Metody uwierzytelniania użytkowników systemu informatycznego przetwarzającego dane osobowe

Każdy użytkownik systemu musi posiadać indywidualny identyfikator oraz hasło dostępu do systemu.

TRYB POSTĘPOWANIA

Logowanie się do systemu

1. Zadaniem logowania jest uniemożliwienie niepowołanego dostępu do systemu informatycznego.
2. Każdy użytkownik systemu informatycznego posiada indywidualny identyfikator oraz hasło dostępu do systemu co jest niezbędne do jego uwierzytelnienia w systemie.
3. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który będzie przetwarzał dane osobowe w systemie informatycznym, odpowiada ASI.
4. Użytkownicy systemu są identyfikowani poprzez tzw. login (krótka nazwa użytkownika – ogólnie znana) i hasło (znane tylko użytkownikowi, ABI oraz ASI).
5. Użytkownik systemu, któremu nie udało się poprawnie zalogować, może po sprawdzeniu poprawności wpisywanych danych ponowić próbę zalogowania.

Hasła dostępu do systemu informatycznego przetwarzającego dane osobowe

1. Każdy użytkownik systemu posiada własne hasło dostępu.
2. Hasło powinno być unikatowe, a jego treść nie powinna umożliwiać identyfikacji użytkownika systemu i musi być zastrzeżona.
3. Użytkownik zobowiązany jest do zachowania w tajemnicy swojego hasła dostępu i nie udostępniania go innym współpracownikom. Zabrania się przechowywania go w postaci zapisanej, w szczególności niedozwolone jest przechowywanie hasła zapisanego np. na obudowie komputera, monitora lub na odwrocie klawiatury.
4. Przy wyborze hasła obowiązują następujące zasady:
    a) minimalna długość hasła – 8 znaków,
    b) zakazuje się stosować:
        - haseł, które użytkownik stosował uprzednio w okresie minionego roku,
        - swojej nazwy użytkownika w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),

- ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego,
- nazwa ulicy na której mieszka lub pracuje, itp.
- wyrazów słownikowych,
- przewidywalnych sekwencji znaków z klawiatury np.: „QWERTY", „12345678",itp.

c) należy stosować:

- hasła zawierające kombinacje liter i cyfr,
- hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp. o ile system informatyczny na to pozwala
- hasła, które można zapamiętać bez zapisywania,
- hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim,

5. Zabronione jest podejmowanie jakichkolwiek prób przywłaszczenia lub rozszyfrowania hasła innego użytkownika.
6. Hasła użytkownika, umożliwiające dostęp do systemu informatycznego, utrzymuje się w tajemnicy również po upływie ich ważności.

5. Rozpoczęcie, zawieszenie i zakończenie pracy przez użytkowników systemu informatycznego przetwarzającego dane osobowe

Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych.

TRYB POSTĘPOWANIA

1. Każdy użytkownik musi przestrzegać warunków i zasad podłączenia sprzętu do sieci, gniazd elektrycznych i logicznych itp. określonych przez Informatyka CUW.
2. Wszelkie zmiany w istniejących podłączeniach bez uprzedniego zezwolenia są niedozwolone.
3. Każdy użytkownik stacji roboczej jest odpowiedzialny za jej stan i bieżącą eksploatację.
4. Przed rozpoczęciem przetwarzania danych użytkownik zobowiązany jest sprawdzić, czy stan pomieszczenia i elementów systemu informatycznego nie wskazuje na możliwość naruszenia bezpieczeństwa danych osobowych, w szczególności:
   - sprawdzić czy na drzwiach i zamkach nie ma widocznych śladów prób niepowołanego ich otwarcia,
   - sprawdzić stan okien i innych zabezpieczeń oraz ocenić czy w pomieszczeniach nie ma znaków wskazujących na przebywanie w osób nieuprawnionych,
   - sprawdzić stan sprzętu informatycznego.
5. Jeśli mogło mieć miejsce naruszenie ochrony danych osobowych, to użytkownik podejmuje działania zgodnie z „Instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych" opisaną w Rozdziale 10 niniejszego dokumentu.
6. Jeśli użytkownik nie wykrył naruszenia zabezpieczeń danych osobowych, to loguje się do systemu za pomocą własnego identyfikatora i hasła.
7. Obowiązkiem użytkownika jest śledzenie reakcji poszczególnych urządzeń i komunikatów pojawiających się na monitorze podczas uruchamiania komputera (stacji roboczej) i bieżącej eksploatacji.
8. W razie wystąpienia nieprawidłowości należy powiadomić ABI.
9. Przed zakończeniem pracy albo przerwą w przetwarzaniu danych użytkownik blokuje dostęp do systemu w sposób uniemożliwiający dostęp do danych bez podania prawidłowego identyfikatora i hasła.
10. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie

identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.

11. W przypadku przerwy w pracy użytkownika stacji roboczej przez okres dłuższy niż 10 minut automatycznie włączany jest wygaszacz ekranu.
12. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.
13. W pomieszczeniach, w których przetwarzane są dane, przebywanie osób nieuprawnionych jest dopuszczalne za zgodą Administratora Danych Osobowych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
14. Po zakończeniu pracy użytkownik zobowiązany jest do przestrzegania poniższych zasad:
    - wylogować się z systemu i poczekać na jego wyłączenie,
    - sprawdzić czy nie zostały pozostawione bez nadzoru nośniki informacji,
    - upewnić się że szafy i biurka z dokumentacją zostały zamknięte.

6. Tworzenie kopii zapasowych zbiorów danych osobowych oraz sposób, miejsce i okres przechowywania elektronicznych nośników informacji

ASI zobowiązany jest do wykonywania kopii awaryjnych zabezpieczających system informatyczny służący do przetwarzania danych osobowych i danych w nim przetwarzanych

TRYB POSTĘPOWANIA

1. Kopie awaryjne wykonywane są w cyklach:
   - dzienna na dysku twardym,
   - miesięczna na płycie CD/DVD.
2. Kopie awaryjne danych wykonuje Administrator Systemu Informatycznego lub osoba przez niego upoważniona.
3. Wzór dziennika ewidencji kopii bezpieczeństwa stanowi **Załącznik nr 5** do niniejszego opracowania.
4. Miesięczne kopie awaryjne na płycie CD/DVD przechowywane są zapieczętowane w kasie pancernej.
5. Kopie awaryjne usuwa się niezwłocznie po ustaniu ich użyteczności.
6. Wzór protokołu zniszczenia stanowi **Załącznik nr 6** do niniejszego opracowania.
7. Urządzenia, dyski lub inne elektroniczne nośniki informacji, 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;
   - przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
   - naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora Danych.
8. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania danych zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

7. Zabezpieczenie systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu

Do ochrony sieci wewnętrznej CUW wykorzystywane jest urządzenie Firewall z funkcjonalnością UTM oraz oprogramowanie antywirusowe z Konsolą centralną którymi zarządza ASI

TRYB POSTĘPOWANIA

1. Do ochrony sieci wewnętrznej CUW wykorzystywane jest urządzenie Firewall z funkcjonalnością UTM (zintegrowane zarządzanie zagrożeniami) oferujące ochronę antyspamową, antywirusową, wykrywanie intruzów, zapobieganie wtargnięciu intruzów, filtrowanie treści internetowych oraz posiadające funkcje zapory ogniowych.
2. Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego.
3. Przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej, system jest chroniony zasilaczami awaryjnymi UPS.
4. Na wszystkich stacjach roboczych zainstalowano oprogramowanie antywirusowe z konsolą centralną zarządzaną przez ASI.
5. Dostęp do programu konfiguracyjnego BIOS zabezpieczony jest hasłem.

8. Sposób odnotowywania informacji o odbiorcach danych osobowych w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych

Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały przekazywane.
Przez odbiorcę danych w myśl art. 7 pkt 6 ustawy rozumie się każdego, komu udostępnia się dane osobowe, z wyłączeniem:

a) osoby, której dane dotyczą,

b) osoby upoważnionej do przetwarzania danych,

c) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

TRYB POSTĘPOWANIA

1. ADO jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały przekazywane.
2. Przez odbiorcę danych w myśl art. 7 pkt 6 ustawy rozumie się każdego, komu udostępnia się dane osobowe, z wyłączeniem:
    a) osoby, której dane dotyczą,
    b) osoby upoważnionej do przetwarzania danych,
    c) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
3. Przekazanie danych osobowych z systemu informatycznego (wydruki z systemu, zewnętrzny nośnik elektroniczny) jest rejestrowane.
4. Pracownik, który udostępnia dane osobowe ma obowiązek prowadzenia rejestrów udostępnionych danych osobowych, który musi zawierać co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję dla której dane udostępniono.

9. Procedury wykonywania przeglądów oraz konserwacji systemu i nośników informacji służących do przetwarzania danych

Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

TRYB POSTĘPOWANIA

1. Wszelkie prace związane z naprawami urządzeń wchodzących w skład systemu informatycznego i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
2. W przypadku uszkodzenia zestawu komputerowego nośnik informacji danych, na których są przechowywane dane osobowe zostaje zabezpieczony przez ASI przed dostępem osób nieuprawnionych.
3. Prace serwisowe na terenie CUW prowadzone w tym zakresie mogą być wykonywane wyłącznie przez pracowników lub przez upoważnionych przedstawicieli wykonawców (serwisantów) zewnętrznych znajdujących się w towarzystwie pracowników CUW.
4. Przedstawiciele wykonawców zewnętrznych muszą posiadać stosowne upoważnienie od ADO.
5. Przed rozpoczęciem prac serwisowych przez osoby spoza CUW konieczne jest potwierdzenie ich tożsamości.
6. W przypadku konieczności przeprowadzenia prac serwisowych poza siedzibą CUW dane z naprawianego urządzenia muszą zostać w sposób trwały usunięte. Od poniższego wymagania możliwe jest odstępstwo, jeżeli urządzenie, podczas przechowywania poza siedzibą CUW, będzie pod stałym nadzorem osoby upoważnionej do dostępu do danych na nim przetwarzanych.

10. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

Instrukcja jest przeznaczona dla osób zatrudnionych przy przetwarzaniu danych osobowych w systemie informatycznym. Instrukcja określa tryb postępowania w przypadkach, gdy:

a) stwierdzono naruszenie zabezpieczenia systemu informatycznego,

b) stan urządzenia, zawartość zbioru danych osobowych, sposób działania aplikacji lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

Każdy kto wykryje naruszenie ochrony danych osobowych przetwarzanych w systemie informatycznym, ma obowiązek niezwłocznie zgłosić to zdarzenie do ABI

TRYB POSTĘPOWANIA

1. Dane osobowe przetwarzane w systemie informatycznym muszą być zabezpieczone przed ich:
   - udostępnieniem osobom nieupoważnionym,
   - zabraniem przez osobę nieuprawnioną,
   - przetwarzaniem z naruszeniem ustawy,
   - zmianą,
   - utratą,
   - uszkodzeniem,
   - zniszczeniem.
2. Przy przetwarzaniu danych osobowych należy dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności związane jest to z zagwarantowaniem, aby dane te były:
   - przetwarzane zgodnie z prawem,
   - zbierane były dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   - merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   - przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
3. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

4. Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym, zobowiązana jest niezwłocznie powiadomić o tym ABI.
5. Każda osoba zatrudniona w CUW, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym, powinna niezwłocznie poinformować o tym osobę zatrudnioną przy przetwarzaniu danych osobowych lub ABI albo inną upoważnioną przez niego osobę.
6. ABI w pierwszej kolejności:
    a. zapisuje wszelkie informacje związane z danym zdarzeniem, a szczególnie: dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,
    b. na bieżąco generuje i drukuje (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, oraz opatruje je datą i podpisem,
    c. przystępuje do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej.
7. Niezwłocznie należy podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji, szczególnie przez:
    a. fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieuprawnionej,
    b. wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,
    c. zmianę hasła dla konta, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.
8. Po wyeliminowaniu bezpośredniego zagrożenia należy przeprowadzić wstępną analizę stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych w systemie.
9. ASI lub inna uprawniona przez niego osoba powinna sprawdzić:
    a. stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
    b. zawartość zbioru danych osobowych,
    c. sposób działania programu,
    d. jakość komunikacji w sieci telekomunikacyjnej,
    e. wykluczyć możliwość obecności wirusów komputerowych.
10. Po dokonaniu powyższych czynności ASI powinien przeprowadzić szczegółową analizę

stanu systemu informatycznego obejmującego identyfikację:

- rodzaju zaistniałego zdarzenia,
- metody dostępu do danych osoby nieuprawnionej,
- skali zniszczeń.

11. Niezwłocznie należy przywrócić normalny stan działania systemu informatycznego, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, niezbędne jest odtworzenie jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego uzyskania dostępu tą samą drogą przez osobę niepowołaną.
12. Po przywróceniu prawidłowego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
13. Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych w systemie informatycznym, należy przeprowadzić dodatkowe szkolenie wszystkich osób biorących udział przy przetwarzaniu danych.
14. Jeżeli przyczyną zdarzenia było uaktywnienie wirusa, należy ustalić źródło jego pochodzenia oraz wykonać zabezpieczenia antywirusowe.
15. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy wyciągnąć konsekwencje regulowane ustawą.
16. Jeżeli przyczyną zdarzenia było włamanie w celu pozyskania bazy danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony bazy danych.
17. Jeżeli przyczyną zdarzenia był zły stan urządzenia lub sposób działania programu, należy wówczas niezwłocznie przeprowadzić kontrolne czynności serwisowo-programowe.
18. ABI przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia (dołączając ewentualne kopie dowodów dokumentujących to zdarzenie) oraz niezwłocznie przekazuje ADO.
19. Prawidłowość ochrony danych osobowych jest weryfikowana w trakcie kontroli prowadzonych przez ABI.

Załączniki

1. Upoważnienie do przetwarzania danych osobowych.
2. Wniosek o nadanie uprawnień do przetwarzania danych osobowych.
3. Indywidualny zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych.
4. Ewidencja osób upoważnionych do przetwarzania danych osobowych.
5. Dziennik ewidencji kopii bezpieczeństwa.
6. Protokół zniszczenia.

Załącznik Nr 1 do Instrukcji

Nowa Sarzyna, dn. ..... r.

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922) upoważniam Panią/ Pana:

.....
Imię i Nazwisko

Pracownika Centrum Usług Wspólnych w Nowej Sarzynie do wykonywania czynności związanych z przetwarzaniem danych osobowych w zakresie:

.....

.....

ze szczególnym uwzględnieniem zadań zawartych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 26 kwietnia 2004r. 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. Nr 100 poz. 1024).

Upoważnienie niniejsze nie upoważnia do udzielania dalszych upoważnień i wygasa z dniem ustania stosunku pracy, a ponadto może być w każdym czasie zmienione lub odwołane. W przypadku posiadania wcześniej wydanych upoważnień niniejsze upoważnienie odwołuje wszystkie uprzednio wydane upoważnienia.

.....
(podpis osoby upoważnionej)

.....
(podpis administratora danych)

Załącznik Nr 2 do Instrukcji

.....
(pieczęć komórki organizacyjnej)

Nowa Sarzyna, dn. ..... r.

WNIOSEK

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
(Dz. U. 2016 r. poz. 922)

wnioskuję o nadanie /pozbawienie/zmianę/*

Pani /Panu/* .....

upoważnienia do przetwarzania danych osobowych w Centrum Usług Wspólnych w Nowej Sarzynie.

Zakres przetwarzania danych osobowych
.....
.....

☐ Dane przetwarzane są w formie papierowej
☐ Dane przetwarzane są w formie elektronicznej

Pracownik może:
☐ Przeglądać dane
☐ Wprowadzać dane
☐ Zmieniać dane
☐ Kasować dane

Upoważnienie wydaje się na okres: /stały/czasowy - do kiedy/*.....

.....
(podpis wnioskującego)

* - niepotrzebne skreślić

INDYWIDUALNY ZAKRES CZYNNOŚCI OSOBY ZATRUDNIONEJ PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Nazwa i adres pracodawcy: Centrum Usług Wspólnych w Nowej Sarzynie

Imię i Nazwisko pracownika: .....

Stanowisko: .....

Przetwarzanie 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 *(art. 7 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2016r. poz. 922).*

Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej *(art. 6 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2016r. poz. 922).*

1) Obowiązkiem każdego pracownika CUW jest zachowanie tajemnicy państwowej i służbowej, również w zakresie ochrony danych osobowych gromadzonych i przetwarzanych przez CUW. Obowiązek ten istnieje również po ustaniu zatrudnienia.
2) Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
3) Dokumentów materialnych (w formie elektronicznej, papierowej itp.) z danymi osobowymi nie można pozostawiać bez dozoru, ani udostępniać osobom nieupoważnionym.
4) Dokumentacji z danymi nie wolno wykorzystywać do innych celów niż służbowe.
5) Dokumentację z danymi nie wolno udostępniać nieuprawnionym.
6) Użytkownik systemu informatycznego musi dopilnować, aby monitor usytuowany był tak, by ekran był niewidoczny dla osób wchodzących do pomieszczenia.
7) Przy krótkotrwałych przerwach w pracy należy stosować blokady stacji roboczych.
8) Pracownik może uzyskać dostęp do systemu informatycznego tylko i wyłącznie jako użytkownik podając swój indywidualny login i hasło.
9) Oprogramowanie wgrywa tylko i wyłącznie Informatyk CUW, nie wolno tego robić samodzielnie.
10) Wydrukowane nadmiarowe, niepotrzebne lub błędne dokumenty należy niezwłocznie, trwale zniszczyć.

OŚWIADCZENIE

1) Oświadczam, że znana jest mi definicja danych osobowych w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2016 r. poz. 922) w myśl, której za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
2) Zostałam/em zaznajomiona/y z przepisami dotyczącymi ochrony danych osobowych, z „Polityką bezpieczeństwa danych osobowych przetwarzanych w Centrum Usług Wspólnych w Nowej Sarzynie" oraz „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Usług Wspólnych w Nowej Sarzynie".
3) Zobowiązuję się, w przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych, bezzwłocznie powiadomić Administratora Bezpieczeństwa Informacji.
4) Zobowiązuję, się przy przetwarzaniu danych osobowych, do szczególnej dbałości o zachowanie poufności, integralności i dostępności danych związanych z dokumentami znajdującymi się w obrocie w CUW, także dotyczących danych osobowych pracowników, dokumentacji systemu przetwarzania danych oraz infrastruktury sprzętowo – programowej systemów informatycznych.
5) Zobowiązuję się przy przetwarzaniu danych, poza systemem informatycznym, do szczególnej dbałości o zachowanie poufności treści dokumentów, które znajdują się w obrocie w Centrum Usług Wspólnych w Nowej Sarzynie oraz przestrzegania zasad dostępu do danych osobowych

Oświadczam, że treść niniejszego zakresu jest mi znana

i zobowiązuję się do jego przestrzegania

Wykonano w 3 egzemplarzach

Potwierdzam odbiór 1 egzemplarza

Nowa Sarzyna, dnia .....

.....

(czytelny podpis pracownika)

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Nazwisko i Imię użytkownika	Identyfikator *	Data nadania upoważnienia	Data ustania upoważnienia

* - wypełnia się w przypadku gdy dane są przetwarzane w systemie informatycznym

Załącznik Nr 5 do Instrukcji

DZIENNIK EWIDENCJI KOPII BEZPECZEŃSTWA

Lp.	Oznaczenie systemu / zbioru danych	Określenie metody (całościowa przyrostowa)	Oznaczenie nośnika, na którym utworzono kopię awaryjną	Kopię bezpieczeństwa utworzył:		
				Nazwisko i Imię administratora	Data	Podpis
1	2	3	4	5	6	7

Załącznik Nr 6 do Instrukcji

.....
(miejscowość, data)

PROTOKÓŁ ZNISZCZENIA

Kopii bezpieczeństwa*/ innych nośników zawierających dane osobowe*

Nr: .....

Komisja w składzie:

1. .....
2. .....
3. .....

Oświadczam, iż kopie bezpieczeństwa* / inne nośniki* otrzymane z .....
(nazwa komórki organizacyjnej)

zostały w dniu ..... komisyjne zniszczone .....

....
(opis procesu zniszczenia)

Rodzaj i oznaczenie nośników:.....

Ilość sztuk: .....

Uwagi: .....

Podpisy komisji:

1. .....
2. .....
3. .....

* niepotrzebne skreślić