SŁUPSKI OŚRODEK KULTURY
76-200 SŁUPSK
ul. Braci Gierymskich 1
tel. 59 845 64 41 59 845 64 42

Zarządzenie nr 08/18
Dyrektora Słupskiego Ośrodka Kultury
z dnia 25 maja 2018 r.
w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Słupskim Ośrodku Kultury

Na podstawie:
- Rozporządzenia Parlamentu Europejskiego i Rady /UE/2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE/Dz. Urz. UW.L nr 119, str.1/;
- ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych

zarządzam, co następuje:

§ 1

Wprowadzam Politykę Bezpieczeństwa w Słupskim Ośrodku Kultury.

§ 2

Zapoznanie się i przestrzeganie zasad niniejszego zarządzenia powierzam wszystkim pracownikom Słupskiego Ośrodka Kultury.

§ 3

Wykonanie zarządzenia powierzam Inspektorowi Ochrony Danych.

§ 4

Zarządzenie wchodzi w życie z dniem 25 maja 2018 r.

DYREKTOR
Słupskiego Ośrodka Kultury
Jolanta Krawczykiewicz

SŁUPSKI OŚRODEK KULTURY
76-200 SŁUPSK
ul. Bracci Clerymskich 1
tel. 59 848 84 41 59 848 84 42

Zarządzenie nr 08/18
Dyrektora Słupskiego Ośrodka Kultury
z dnia 25 maja 2018 r.
w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych Osobowych
w Słupskim Ośrodku Kultury

Na podstawie:
- Rozporządzenia Parlamentu Europejskiego i Rady (UE)2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE(Dz. Urz. UWLL nr 119, str.1);
- ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

zarządzam, co następuje:

§ 1

Wprowadzam Politykę Bezpieczeństwa w Słupskim Ośrodku Kultury.

§ 2

Zapoznanie się i przestrzeganie zasad niniejszego zarządzenia powierzam wszystkim pracownikom Słupskiego Ośrodka Kultury.

§ 3

Wykonanie zarządzenia powierzam Inspektorowi Ochrony Danych.

§ 4

Zarządzenie wchodzi w życie z dniem 25 maja 2018 r.

DYREKTOR
Słupskiego Ośrodka Kultury
Jolanta Krzyżanowska

Polityka bezpieczeństwa przetwarzania danych osobowych w Słupskim Ośrodku Kultury

Rozdział 1
Postanowienia ogólne

§ 1

Celem Polityki bezpieczeństwa przetwarzania danych osobowych, zwanej dalej „Polityką bezpieczeństwa" w Słupskim Ośrodku Kultury, zwanej dalej „Organizacją", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe.

§ 2

Polityka bezpieczeństwa została opracowana w oparciu o wymagania zawarte w:

- Rozporządzeniu Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str.1/,
- Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych

§ 3

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników proporcjonalne i adekwatne do ryzyka naruszenia bezpieczeństwa danych osobowych przetwarzanych w ramach prowadzonej działalności.

§ 4

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w Organizacji rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest akceptowalna wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
    1. poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
    2. integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
    3. rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
    4. integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
    5. dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
    6. zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które

może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 5

1. Administratorem danych osobowych przetwarzanych w Słupskim Ośrodku Kultury jest Dyrektor SOK – Jolanta Krawczykiewicz
2. Administrator danych osobowych powołał inspektora ochrony danych, zgodnie art. 37 RODO. Zadania inspektora ochrony danych zawarte są w art. 39 RODO oraz

Rozdział 2
Definicje

§ 6

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1. **administrator danych osobowych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
2. **inspektor ochrony danych** – osoba wyznaczona przez administratora danych osobowych, nadzorująca przestrzeganie zasad i wymogów ochrony danych osobowych określonych w RODO i przepisach krajowych,
3. **ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych
4. **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 /Dz. Urz. UE.L nr 119, str. 1/,
5. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,
6. **zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów,
7. **przetwarzane danych** – operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, łączenie, przesyłanie, zmienianie, udostępnianie i usuwanie, niszczenie, itd.,
8. **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych,
9. **system tradycyjny** – zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenie i środki trwałe wykorzystywane w celu przetwarzania danych osobowych na papierze,
10. **zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

11. **administrator systemu informatycznego** – osoba lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi,
12. **odbiorca** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe w oparciu m. in. o umowę powierzenia,
13. **strona trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, które z upoważnienia administratora danych osobowych mogą przetwarzać dane osobowe,
14. **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
15. **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Rozdział 3
Zakres stosowania

§ 7

1. W Organizacji przetwarzane są dane osobowe pracowników, kandydatów do pracy, wolontariuszy, stażystów, praktykantów, klientów, uczestników zajęć/warsztatów/konkursów zebrane w zbiorach danych osobowych.
2. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
3. Polityka bezpieczeństwa zawiera uregulowania dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
4. Innymi dokumentami regulującymi ochronę danych osobowych w Organizacji są:
    1. instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Organizacji,
    2. ewidencja osób upoważnionych do przetwarzania danych osobowych,
    3. procedura postępowania w przypadku naruszenia ochrony danych osobowych,
    4. rejestr czynności przetwarzania
    5. rejestr kategorii czynności przetwarzania

§ 8

Politykę bezpieczeństwa stosuje się w szczególności do:

1. danych osobowych przetwarzanych w systemie: Gratyfikant GT, Rewizor GT, Subiekt GT, Płatnik, Aplikacji Ekobilet, Aplikacji eRU.
2. wszystkich informacji dotyczących danych pracowników, klientów, uczestników zajęć/warsztatów, wolontariuszy, praktykantów, stażystów
3. odbiorców danych osobowych, którym przekazano dane osobowe do przetwarzania w oparciu o umowy powierzenia

4. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5. rejestru osób trzecich mających upoważnienia administratora danych osobowych do przetwarzania danych osobowych,
6. innych dokumentów zawierających dane osobowe.

§ 9

1. Zakresy ochrony danych osobowych określone przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty mają zastosowanie do:
    1. wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie,
    2. wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
    3. wszystkich pracowników, stażystów, praktykantów, wolontariuszy i innych osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez Politykę bezpieczeństwa oraz inne z nią związane dokumenty zobowiązani są wszyscy pracownicy, stażyści, praktykanci, wolontariusze oraz inne osoby mające dostęp do danych osobowych podlegających ochronie.

Rozdział 4
Wykaz zbiorów danych osobowych

§ 10

1. Dane osobowe gromadzone są w zbiorach

1. Akta osobowe pracowników,
2. Zbiory informacji o pracownikach,
3. Ewidencja zwolnień lekarskich,
4. Skierowania na badania okresowe, specjalistyczne,
5. Ewidencja urlopów, czasu pracy, wyjść,
6. Listy płac pracowników,
7. Deklaracje ubezpieczeniowe pracowników,
8. Deklaracje i kartoteki ZUS pracowników,
9. Deklaracje podatkowe pracowników,
10. Deklaracje ubezpieczenia grupowego pracowników,
11. Dokumenty ZFŚS
12. Newsletter
13. Monitoring
14. Umowy cywilno-prawne,
15. Umowy zawierane z kontrahentami,

16. Dokumenty archiwalne,
17. Dokumenty Pracowniczej Kasy Zapomogowo-Pożyczkowej,
18. Umowy wolontarystyczne
19. Ewidencja osób upoważnionych do przetwarzania danych osobowych,
20. Rejestr delegacji służbowych,
21. Rejestr wypadków,
22. Polecenia pracy,
23. Dokumenty pracowników – cudzoziemców,
24. Umowy o stażu i praktykach zawodowych
25. Nabór kandydatów do pracy
26. Dane archiwum

§ 11

Zbiory danych osobowych wymienione w § 10 ust. w pkt. 1-11 podlegają przetwarzaniu w sposób tradycyjny i przy użyciu systemu informatycznego, zbiory określone w pkt. 12-13 przetwarzane są przy pomocy systemu informatycznego, a zbiory określone w pkt. 14-26 gromadzone są i przetwarzane w sposób tradycyjny

Rozdział 5
Wykaz budynków, pomieszczeń, w których wykonywane są operacje przetwarzania danych osobowych

§ 12

1. Dane osobowe przetwarzane są w budynkach, mieszczącym się w:
   - **Słupskim Ośrodku Kultury przy ulicy Braci Gierymskich 1 (Główna siedziba)**

1.	pomieszczenia, w których przetwarzane są dane osobowe	*Sekretariat, pokój nr 5, Pracownia batiku*
2.	pomieszczenia, w których znajdują się komputery stanowiące element systemu informatycznego	*Sekretariat, Gabinet Dyrekcji, pokój nr 3,5, Pracownia Muzyczna*
3.	Pomieszczenia, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe	*Sekretariat – kadry; pokój nr 5, Pracownia batiku – dzienniki lekcyjne*
4.	pomieszczenia archiwum	*pokój nr 5, Archiwum w kondygnacji 0*

   - **Ośrodku Teatralnym Rondo przy ul. M. Niedziałkowskiego 5a**

1.	pomieszczenia, w których przetwarzane są dane osobowe	*Księgowość, Pokój instruktorski, Pracownia fotograficzna*
2.	pomieszczenia, w których znajdują się komputery stanowiące element systemu informatycznego	*Pomieszczenie Serwerowe, Pomieszczenie techniczne, Pokój instruktorski, Pokój stowarzyszeń, Pracownia fotograficzna, ciemnia*

		fotograficzna, księgowość, gabinet Dyrekcji
3.	Pomieszczenia, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe	*Pomieszczenie Serwerowe, księgowość – kadry i płace* *Pokój instruktorski, Pracownia fotograficzna – dzienniki lekcyjne,*
4.	pomieszczenia, w których składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, dyski przenośne, uszkodzone komputery)	*Pomieszczenie techniczne*

- **Pracowni Ceramicznej przy al. Wojska Polskiego 10a**

1.	pomieszczenia, w których przetwarzane są dane osobowe	*Pracownie zajęciowe kondygnacji 0 i 1 – dzienniki lekcyjne*
2.	pomieszczenia, w których znajdują się komputery stanowiące element systemu informatycznego	*Pomieszczenie socjalne/gabinet kierownika administracyjnego*
2.	Pomieszczenia, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe)	*Pracownie zajęciowe kondygnacji 0 i 1*

- **Emceku przy al. 3 Maja 22**

1.	pomieszczenia, w których przetwarzane są dane osobowe	*Sekretariat, pokój 20, 23, 25, Dział filmowy, Pracownia Muzyczna*
2.	pomieszczenia, w których znajdują się komputery stanowiące element systemu informatycznego	Kabina projekcyjna, Pracownia muzyczna, pokój 15,21,22,23,24
3.	Pomieszczenia, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe)	*Kabina projekcyjna*
4.	pomieszczenia, w których składowane są uszkodzone komputerowe nośniki	*Kabina projekcyjna*

	danych (taśmy, dyski, płyty CD, dyski przenośne, uszkodzone komputery)	
5.	pomieszczenia archiwum	Archiwum na parterze

Rozdział 6
Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

§ 13

Lp.	Zbiór danych	Dział	Program	Lokalizacja bazy danych	Miejsce przetwarzania danych
1.	Dane pracowników	Kadry	Gratyfikant GT	Serwer (O.T. Rondo)	Sekretariat SOK ul. Braci Gierymskich 1
2.	Dane pracowników	Księgowość	Gratyfikant GT	Serwer (O.T. Rondo)	Księgowość O.T. Rondo ul. M. Niedziałkowskiego 5a
3.	Dane pracowników	Księgowość	Rewizor GT	Serwer (O.T. Rondo)	Księgowość O.T. Rondo ul. M. Niedziałkowskiego 5a
4.	Dane kontrahentów	Księgowość	Subiekt GT	Serwer (O.T. Rondo)	Księgowość O.T. Rondo ul. M. Niedziałkowskiego 5a
5.	Dane pracowników	Księgowość	Płatnik	Serwer (O.T. Rondo)	Księgowość O.T. Rondo ul. M. Niedziałkowskiego 5a
6.	Dane monitoringu	Administracja	Hikvision DVR/NVR	HDD (O.T. Rondo)	Serwerownia Rondo ul. M. Niedziałkowskiego 5a
7.	Newsletter	Public relations/Dział filmowy	Aplikacja pocztowa home.pl/panel zarządzania stroną www.sok.slupsk.pl	Serwer wirtualny sok.slups.pl	Office O.T. Rondo ul. M. Niedziałkowskiego 5a/ Dział filmowy Emcek al. 3 Maja 22
6.	Dane osób płącących za bilety kinowe online	Dział Filmowy	Aplikacja Ekobilet	Serwer aplikacji Ekobilet	Dział filmowy Emcek al. 3 Maja 22

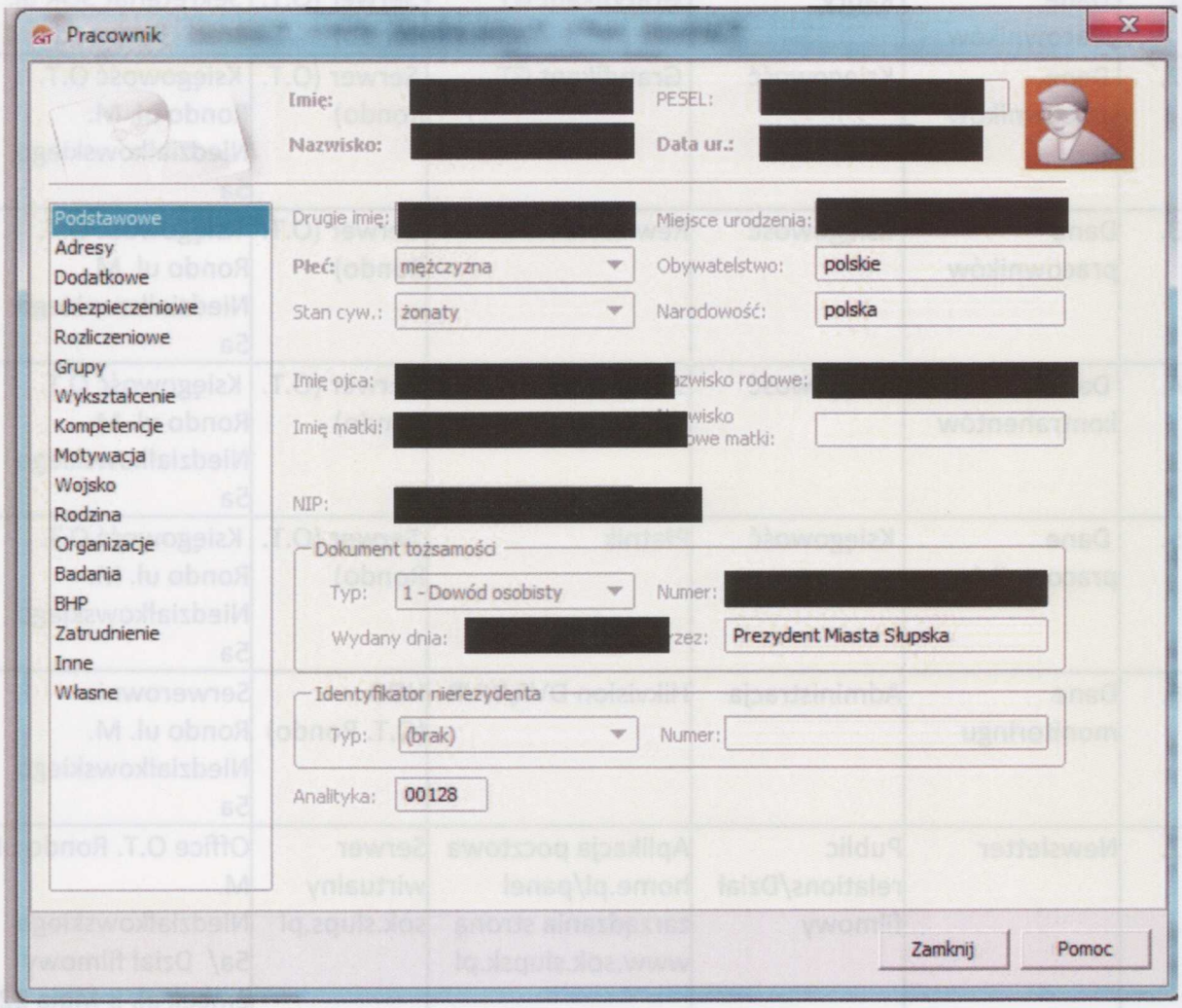
	(dane procesowane w ramach umowy powierzenia)				

Rozdział 7
Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych

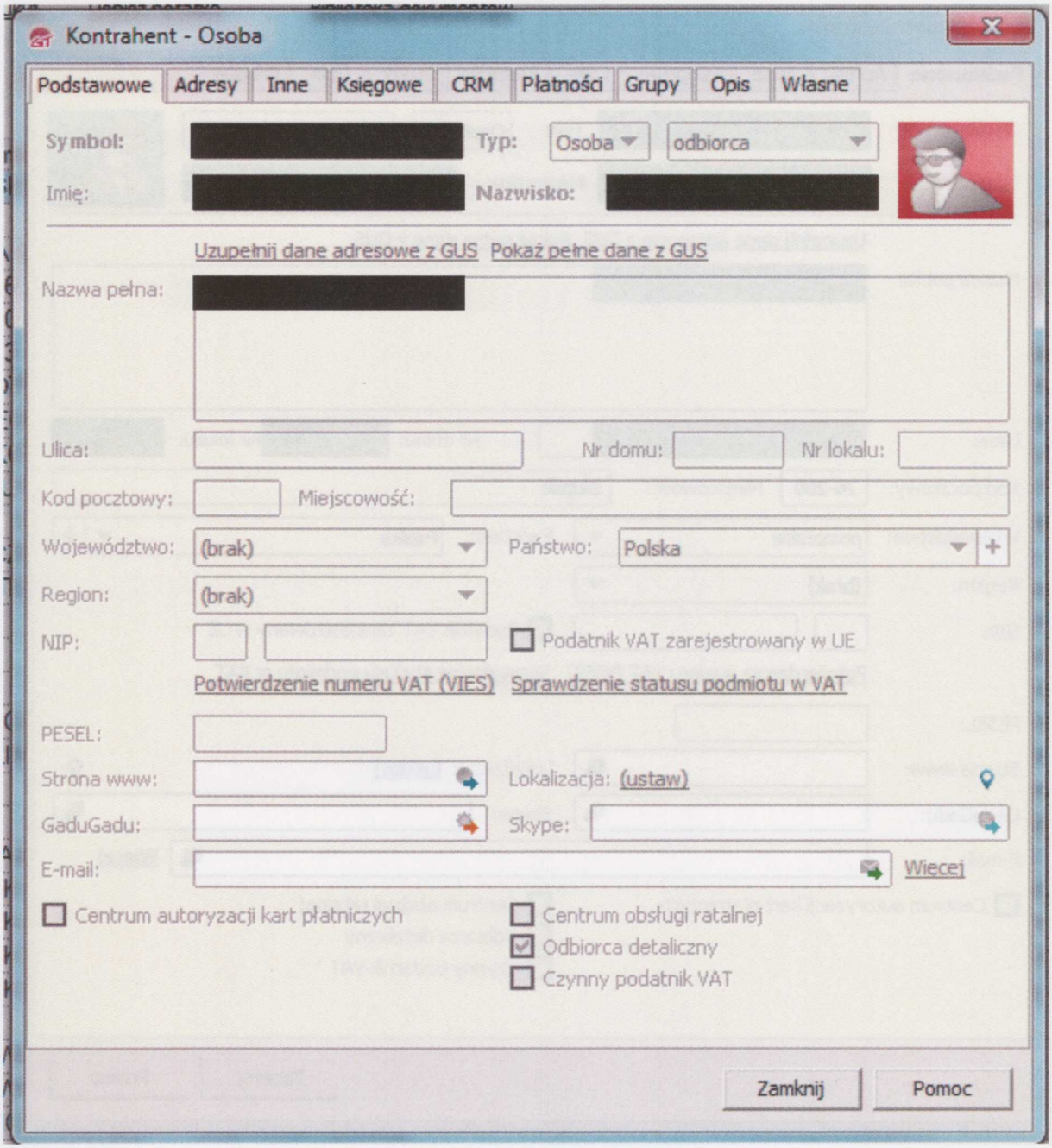
§ 14

Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych dla programów i systemów stosowanych w Organizacji przedstawia się w sposób następujący:

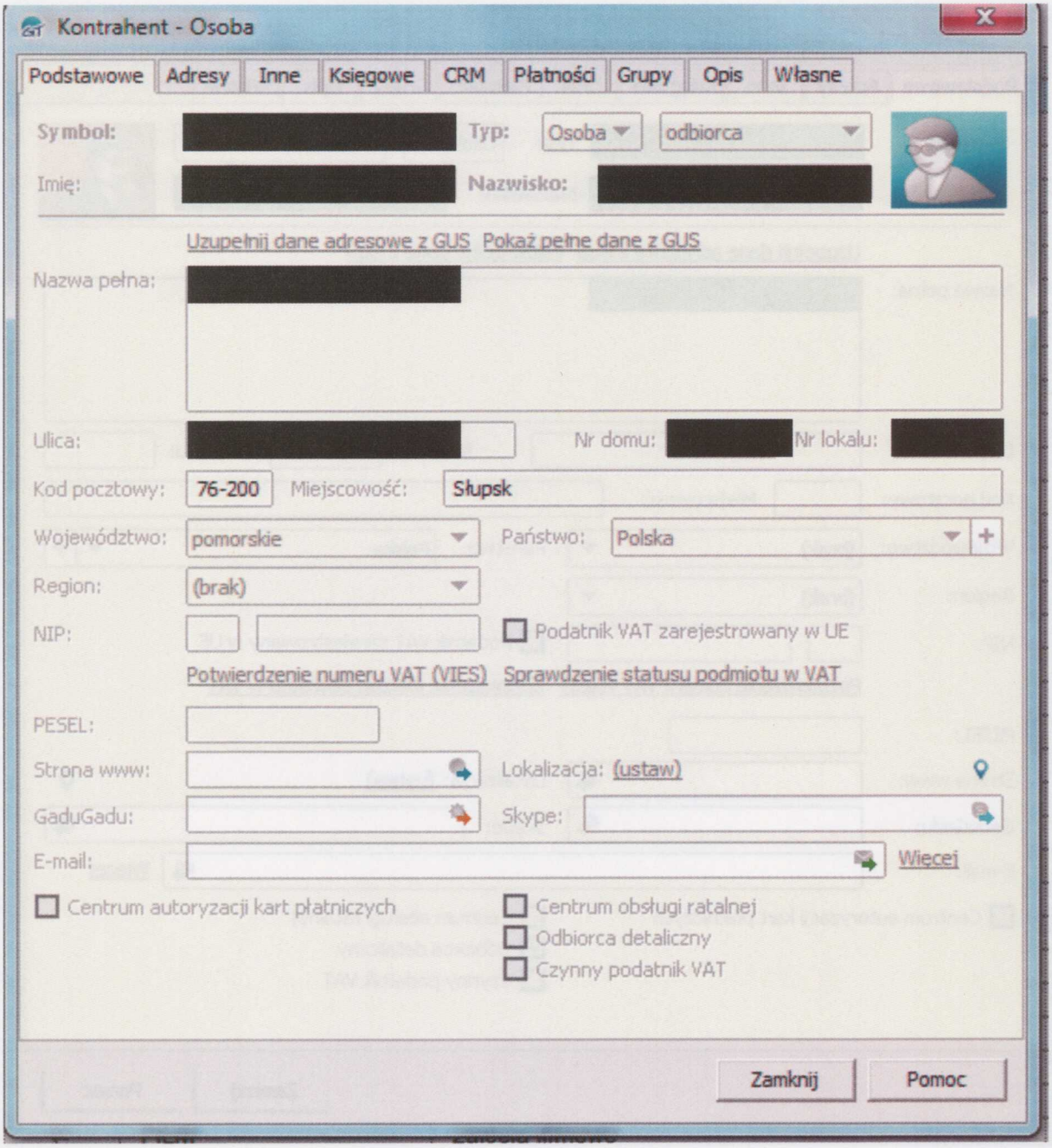
Program: Gratyfikant GT



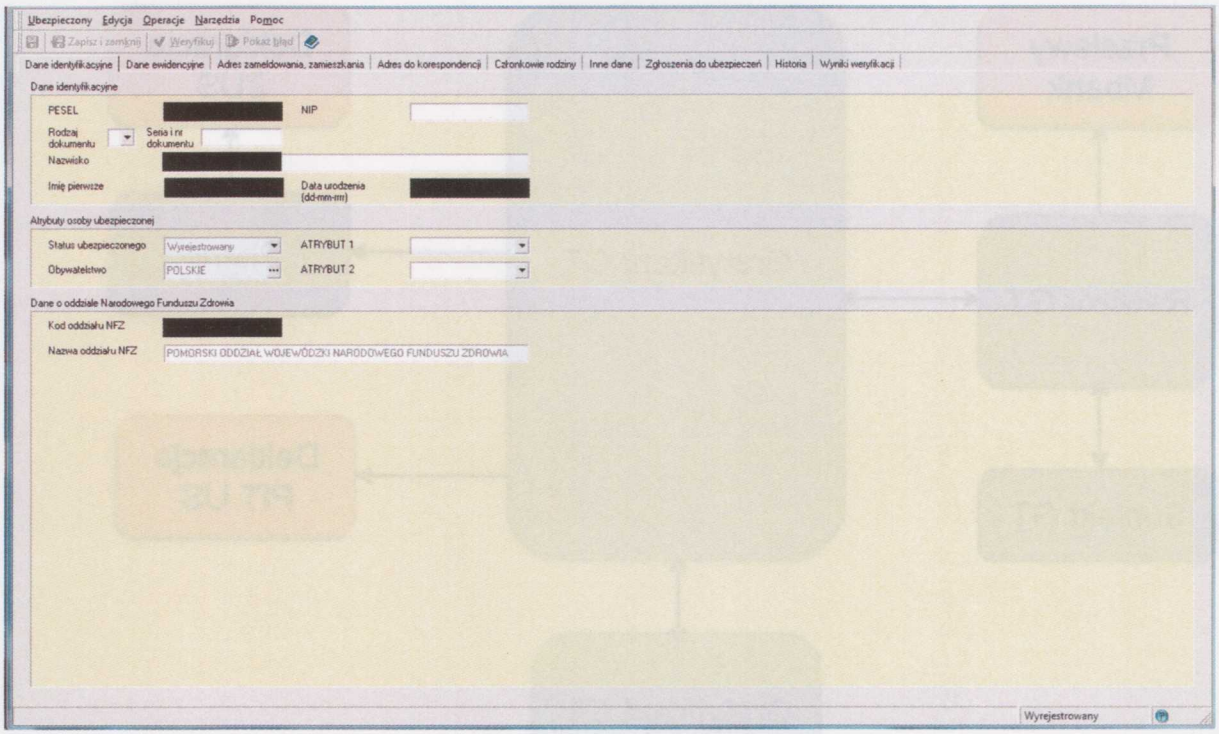
Program: Rewizor GT



Program: Subiekt GT



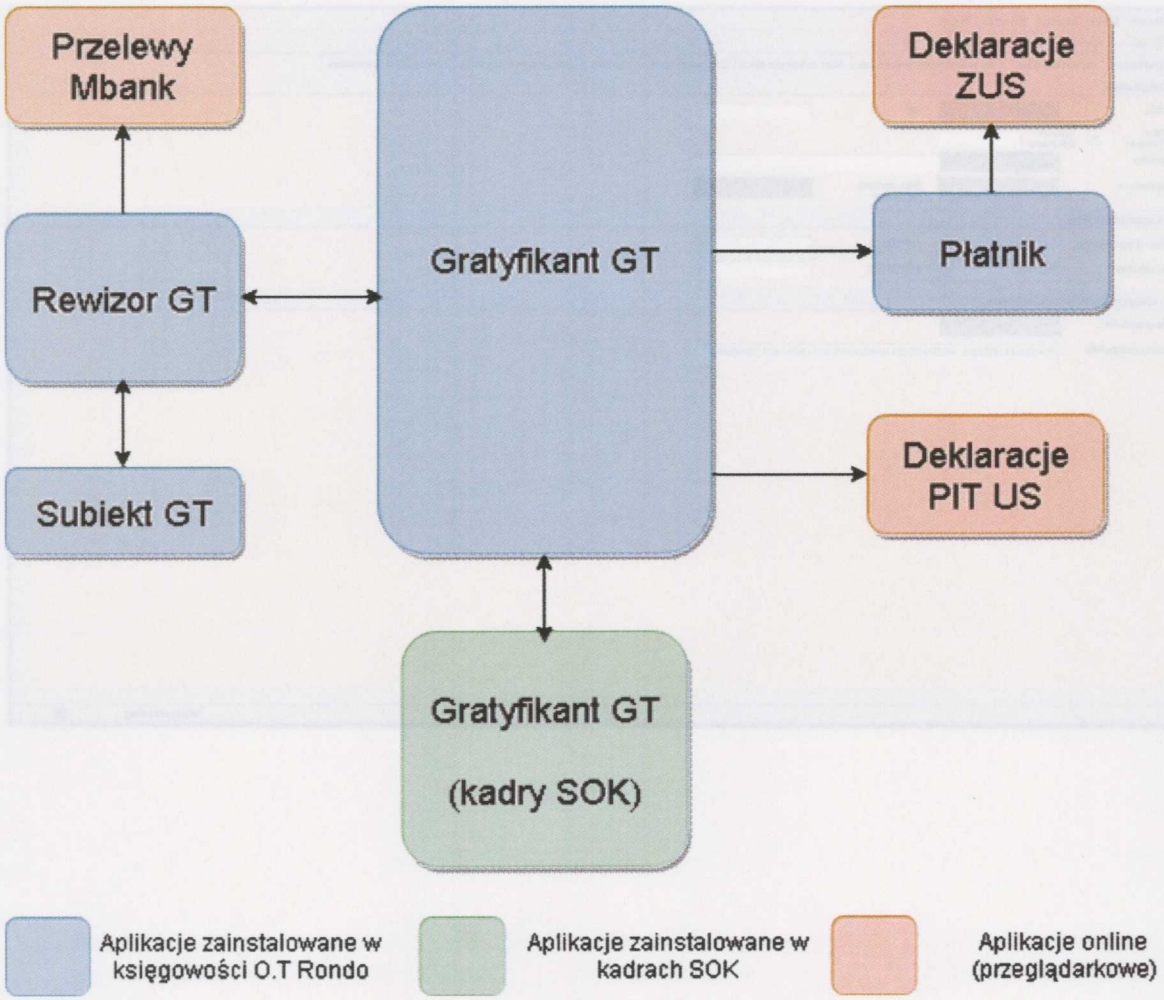
Program: Płatnik



Rozdział 8
Sposób przepływu danych między poszczególnymi systemami, współpracy systemów informatycznych ze zbiorami danych

§ 15

Przepływ danych pomiędzy poszczególnymi systemami kadrowo-księgowymi



Rozdział 9
Środki organizacyjne i techniczne zabezpieczenia danych osobowych

§ 16

1. Zabezpieczenia organizacyjne

    1. opracowano i wdrożono Politykę bezpieczeństwa przetwarzania danych osobowych,
    2. sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Organizacji,
    3. stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych,
    4. opracowano i bieżąco prowadzi się rejestr czynności przetwarzania
    5. wyznaczono inspektora ochrony danych,
    6. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych bądź osobę przez niego upoważnioną,

7. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
8. osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
9. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
10. przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
11. dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonuje się takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści.

2. Zabezpieczenia techniczne

1. wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą sprzętowego firewalla, Bramy DNS oraz filtrowania MAC
2. stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
3. komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania

3. Środki ochrony fizycznej:

1. obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest alarmem,
2. Budynek O.T. Rondo objęty jest całodobowym monitoringiem,
3. urządzenia służące do przetwarzania danych osobowych umieszczone są w zamykanych pomieszczeniach,
4. dokumenty i nośniki informacji zawierające dane osobowe przechowywane są w zamykanych na klucz szafach.

Rozdział 10
Zadania inspektora ochrony danych

§ 17

Do najważniejszych obowiązków inspektora ochrony danych

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami RODO i ustawy o ochronie danych osobowych,
2. zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki bezpieczeństwa i innymi dokumentami wewnętrznymi,
3. przeprowadzenie oceny skutków planowanej operacji przetwarzania dla ochrony danych osobowych – w przypadku, gdy organizacja wprowadza nowy rodzaj przetwarzania danych osobowych,

4. wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
5. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
6. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
7. nadzór nad bezpieczeństwem danych osobowych,
8. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
9. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

Rozdział 11
Zadania administratora systemu informatycznego

§ 18

1. Administrator systemu informatycznego odpowiedzialny jest za:
    1. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
    2. optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego,
    3. instalacje i konfiguracje oprogramowania systemowego, sieciowego,
    4. konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem,
    5. nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
    6. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
    7. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
    8. zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
    9. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
    10. przyznawanie na wniosek administratora danych osobowych lub inspektora ochrony danych ściśle określonych praw dostępu do informacji w danym systemie,
    11. wnioskowanie do administratora danych osobowych lub inspektora ochrony danych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
    12. zarządzanie licencjami, procedurami ich dotyczącymi,
    13. prowadzenie profilaktyki antywirusowej.
2. Praca administratora systemu informatycznego jest nadzorowana pod względem przestrzegania RODO, ustawy o ochronie danych osobowych, oraz Polityki bezpieczeństwa Organizacji przez administratora danych lub inspektora ochrony danych.

Rozdział 12
Sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych

§ 19

1. Corocznie do dnia 31 grudnia inspektor ochrony danych przygotowuje sprawozdanie roczne z funkcjonowania systemu ochrony danych osobowych i przekazuje do administratora danych osobowych.
2. Sprawozdanie przygotowywane jest w formie pisemnej.

Rozdział 13
Postanowienia końcowe

§ 20

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada inspektor ochrony danych
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką bezpieczeństwa i innymi związanymi z nią dokumentami obowiązującymi u administratora danych osobowych,
4. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.

Załączniki:

1. Instrukcja zarządzania systemem informatycznym w Słupskim Ośrodku Kultury
2. Procedura postępowania w przypadku naruszenia ochrony danych osobowych w Słupskim Ośrodku Kultury
3. Rejestr czynności przetwarzania w Słupskim Ośrodku Kultury
4. Rejestr kategorii czynności przetwarzania w Słupskim Ośrodku Kultury

DYREKTOR
Słupskiego Ośrodka Kultury
Jolanta Krawczykiewicz

DYREKTOR
Słupskiego Ośrodka Kultury
Jolanta Krupczyńska-Iwicz

Załącznik nr 1
do Polityki bezpieczeństwa przetwarzania
danych osobowych w Słupskim Ośrodku Kultury

Instrukcja zarządzania systemem informatycznym w Słupskim Ośrodku Kultury

Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych Słupskiego Ośrodka Kultury przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Definicje:

1. **Administrator Danych** – Słupski Ośrodek Kultury ul. Braci Gierymskich 1, 76-200 Słupsk
2. **Dane osobowe** – wszelkie informacje, w tym o stanie zdrowia, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
3. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych
4. **Użytkownik** – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych w Słupskim Ośrodku Kultury
5. **Sieć lokalna** – połączenie Systemów informatycznych Administratora Danych wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych
6. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie
7. **Przetwarzanie danych** – 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
8. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym Przetwarzaniem
9. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do Przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie
10. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym (Użytkownikowi)

I. Procedury nadawania uprawnień do Przetwarzania danych i rejestrowania tych uprawnień w Systemie informatycznym

1. Za bezpieczeństwo Danych osobowych w Systemie informatycznym Słupskiego Ośrodka Kultury i za właściwy nadzór odpowiedzialny jest Administrator Danych
2. Do obsługi Systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do Przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez Administratora Danych
3. Po upoważnieniu osoby do dostępu do przetwarzania danych osobowych w systemie informatycznym zostaje jej nadany Identyfikator użytkownika. Z chwilą nadania Identyfikatora osoba może uzyskać dostęp do systemów informatycznych w zakresie odpowiednim do danego upoważnienia.
4. Dla każdego Użytkownika Systemu informatycznego ustalony jest odrębny Identyfikator i Hasło.
5. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu Użytkownika z Systemu informatycznego nie może być przydzielony innej osobie.
6. Identyfikator osoby, która utraciła uprawnienia do dostępu do Danych osobowych, zostaje niezwłocznie wyrejestrowany z Systemu informatycznego, w którym są przetwarzane, zaś Hasło dostępu zostaje unieważnione oraz zostają podjęte inne działania niezbędne w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

II. Metody i środki Uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. W Systemie informatycznym stosuje się Uwierzytelnianie na poziomie dostępu do systemu operacyjnego oraz na poziomie dostępu do programów. Do Uwierzytelnienia Użytkownika na poziomie dostępu do systemu operacyjnego oraz do programu stosuje się Hasło oraz Identyfikator użytkownika.
2. Hasła użytkowników umożliwiające dostęp do Systemu informatycznego utrzymuje się w tajemnicy również po upływie ich ważności.
3. Minimalna długość Hasła przydzielonego Użytkownikowi wynosi 8 znaków alfanumerycznych i znaków specjalnych.
4. Zabrania się używania identyfikatora lub Hasła drugiej osoby.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez Użytkowników systemu

1. Pracownik po przyjściu do pracy uruchamia stację roboczą.
2. Przed uruchomieniem komputera należy sprawdzić, czy nie zostały do niego podłączone żadne niezidentyfikowane urządzenia.
3. Po uruchomieniu pracownik loguje się przy pomocy identyfikatora Użytkownika oraz hasła do systemu informatycznego.
4. W trakcie pracy przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane Dane osobowe.

5. Przy opuszczaniu stanowiska na dłuższy czas należy ustawić ręcznie blokadę klawiatury i wygaszacz ekranu (wygaszacz nie rzadszy niż aktywujący się po 15 min braku aktywności).

IV. Tworzenie kopii zapasowych Zbiorów danych

1. Dla zabezpieczenia integralności danych dokonuje się archiwizacji danych w systemach.
2. Do archiwizacji służą dyski zewnętrzne przechowywane przez administratora systemu informatycznego
3. Wszystkie dane archiwizowane winny być identyfikowane, tj. zawierać takie informacje jak datę dokonania zapisu oraz identyfikator zapisanych w kopii danych.

V. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających Dane osobowe oraz kopii zapasowych

1. Nośniki z kopiami archiwalnymi powinny być zabezpieczone przed dostępem do nich osób nieupoważnionych, przed zniszczeniem czy kradzieżą.
2. Nośników z danymi zarchiwizowanymi nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są Zbiory danych osobowych używane na bieżąco.
3. Nośniki informacji, kopie zapasowe, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
4. Kopie, które są już nieprzydatne, należy zniszczyć fizycznie lub stosując wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane kasowane.
5. Zabrania się wynoszenia jakichkolwiek nagranych nośników zawierających dane osobowe z miejsca pracy.

VI. Sposób zabezpieczenia Systemu informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awariami zasilania

1. System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej.
2. Ruch w sieci informatycznej jest zabezpieczony za pomocą zapory sieciowej. Ruch jest monitorowany przez Administratora Systemu Informatycznego w celu kontroli przepływu danych między siecią publiczną, a siecią Administratora Danych oraz kontroli działań w sieciach.
3. Poczta elektroniczna jest zabezpieczona przed przesyłaniem niezamówionej informacji handlowej (tzw. *SPAM*) oraz oprogramowania złośliwego za pomocą filtrów poczty.

4. Na wszystkich stacjach roboczych oraz serwerach zainstalowane jest oprogramowanie antywirusowe ESET Endpoint Seciurity
5. Użytkowany system jest automatycznie skanowany z częstotliwością dzienną
6. Aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy.
7. W przypadku wykrycia wirusa należy:
    a. uruchomić program antywirusowy i skontrolować użytkowany system,
    b. usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego.

    Jeżeli operacja usunięcia wirusa się nie powiedzie, należy:
    c. zakończyć pracę w systemie komputerowym,
    d. odłączyć zainfekowany komputer od sieci,
    e. powiadomić o zaistniałej sytuacji Administratora Danych lub Inspektora Ochrony Danych
8. Urządzenia i nośniki zawierające Dane osobowe przekazywane poza obszar, w którym są one przetwarzane, zabezpiecza się w sposób zapewniający poufność i integralność danych.

VII. Poczta elektroniczna

Pracownicy mogą korzystać z poczty elektronicznej w celach służbowych oraz w celach prywatnych w zakresie ograniczonym swoimi obowiązkami.

1. Administrator może poznawać treść wiadomości elektronicznych wykorzystywanych przez pracowników znajdujących się we wszystkich systemach Administratora.
2. Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem (tzw. *phishing e-mail*).
3. W szczególności zabronione jest otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.

VIII. Sposoby realizacji w systemie wymogów dotyczących Przetwarzania danych

(sposób realizacji wymogu zapisania w Systemie informatycznym informacji o odbiorcach danych)

1. Informacje o odbiorcach danych zapisywane są w Systemie informatycznym, z którego nastąpiło udostępnienie.
2. Informacja o odbiorcy danych zapisana jest w Systemie informatycznym przy uwzględnianiu daty i zakresu udostępnienia, a także dokładnego określenia odbiorcy danych.
3. Możliwe jest sporządzenie i wydrukowanie raportu zawierającego, w powszechnie zrozumiałej formie, powyższe informacje.

IX. Procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do Przetwarzania danych

Przeglądy kontrolne, serwis sprzętu i oprogramowania powinny być dokonywane przez osoby do tego upoważnione oraz przez firmy serwisowe, z którymi zostały zawarte umowy zawierające postanowienia zobowiązujące je do przestrzegania zasad poufności informacji uzyskanych w ramach wykonywanych zadań.

1. Przy dokonywaniu serwisu należy przestrzegać następujących zasad:
    a. czynności serwisowe powinny być wykonywane w obecności osoby upoważnionej do Przetwarzania danych,
    b. przed rozpoczęciem tych czynności dane i programy znajdujące się w systemie powinny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą,
    c. w przypadku prac serwisowych dokonywanych przez podmiot zewnętrzny, wymagających dostępu do Danych osobowych, z podmiotem takim powinny zostać zawarte stosowne umowy powierzenia danych osobowych.

Załącznik nr 2
do Polityki bezpieczeństwa przetwarzania
danych osobowych w Słupskim Ośrodku Kultury

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Słupskim Ośrodku Kultury

Istota naruszenia danych osobowych

§ 1

Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

- nieautoryzowany dostęp do danych,
- nieautoryzowane modyfikacje lub zniszczenie danych,
- udostępnienie danych nieautoryzowanym podmiotom,
- nielegalne ujawnienie danych,
- pozyskiwanie danych z nielegalnych źródeł.

Postępowanie w przypadku naruszenia danych osobowych

§ 2

1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt Inspektorowi ochrony danych.
2. Typowe sytuacje, gdy użytkownik powinien powiadomić Inspektora ochrony danych:
    a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
    b. dokumentacja jest niszczona bez użycia niszczarki;
    c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
    d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.
    e. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych,

f. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;

g. wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia;

h. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;

i. stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);

j. telefoniczne próby wyłudzenia danych osobowych;

k. kradzież komputerów lub twardych dysków z danymi osobowymi;

l. utrata kontroli nad kopią danych osobowych;

m. maile zachęcające do ujawnienia identyfikatora i/lub hasła;

n. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;

o. istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki"

p. hasła do systemów przechowywane są w pobliżu komputera.

§ 3

Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia .

§ 4

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora ochrony danych lub innej osoby upoważnionej przez Administratora danych.

§ 5

Administrator Systemu Informatycznego jest zobowiązany do informowania Inspektora ochrony danych o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

§ 6

Inspektor ochrony danych podejmuje następujące kroki:

- zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
- odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
- nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

§ 7

Inspektor ochrony danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport - Załącznik nr 1.

§8

Inspektor ochrony danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych) - Załącznik nr 2 - rejestr incydentów i działań korygujących i zapobiegawczych

Naruszenie danych osobowych - odpowiedzialność

§ 9

1. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

§ 10

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi ochrony danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia – Załącznik nr 3.
2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
    1. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
    2. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
    3. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
    4. opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte

działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

§ 11

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w § 10 ust. 2 pkt. 1,2 i 3.
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
    1. administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
    2. administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
    3. wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób

Załączniki:

Załącznik nr 1. Raport z naruszenia ochrony danych

1. Data ..... Godzina .....

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):

.....

3. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

.....

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

.....

5. Podjęte działania:

.....

6. Wstępna ocena przyczyn wystąpienia naruszenia:

.....

7. Postępowanie wyjaśniające i naprawcze:

.....

(podpis pracownika) (data i podpis Inspektora ochrony danych)

Załącznik nr 2. Rejestr incydentów bezpieczeństwa i działań korygujących i zapobiegawczych

Rejestr incydentów bezpieczeństwa i działań korygujących i zapobiegawczych								
Incydent	**Źródło zgłoszenia**	**Data rozpoczęcia**	**Data zakończenia**	**Czy koniec?**	**Odpowiedzialny za realizację**	**Przyczyna niezgodności**	**Działanie korygujące / zapobiegawcze**	**Ocena skuteczności**
podać opis incydentu	podać źródło zgłoszenia np. zawiadomienie, kontrola, itd.			czy incydent się zakończył Tak/Nie	podać dane osoby lub funkcje osoby odpowiedzialnej	podać przyczynę powstania incydentu	opisać działania jakie podjęto w celu przywrócenia bezpieczeństwa	opisać jakie skutki przyniosło działanie korygujące

Załącznik nr 3. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

1. Data ..... Godzina .....(naruszenia)

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):

.....

3. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

.....

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu (*opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie);*

.....

5. Podjęte działania:

.....

6. Wstępna ocena przyczyn wystąpienia naruszenia (*opisywać możliwe konsekwencje naruszenia ochrony danych osobowych);*

.....

7. Postępowanie wyjaśniające i naprawcze (*opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków);*

.....

8. Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji:

.....

(data i podpis administratora)