

Załącznik Nr 1  
do Zarządzenia Nr 51  
Mazowieckiego Kuratora Oświaty  
z dnia 14 czerwca 2012 r.

**POLITYKA BEZPIECZEŃSTWA**  
**DANYCH OSOBOWYCH**  
**W KURATORIUM OŚWIATY W WARSZAWIE**

## Spis treści

Stosowane definicje .....	3
Część 1. Cel i zakres polityki bezpieczeństwa .....	4
Część 2. Deklaracja Administratora danych osobowych .....	4
Część 3. Podstawowe zasady ochrony danych osobowych .....	4
Część 4. Sposób przetwarzania danych osobowych .....	7
<i>Rozdział 1. Obszar przetwarzania danych osobowych .....</i>	<i>7</i>
<i>Rozdział 2. Wykaz zbiorów danych osobowych i programów wykorzystywanych do przetwarzania danych osobowych .....</i>	<i>7</i>
<i>Rozdział 3. Poziom bezpieczeństwa przetwarzania danych osobowych .....</i>	<i>7</i>
<i>Rozdział 4. Opis struktury zbiorów danych osobowych .....</i>	<i>7</i>
<i>Rozdział 5. Sposób przepływu danych pomiędzy poszczególnymi systemami .....</i>	<i>7</i>
<i>Rozdział 6. Środki zapewniające poufność, integralność, dostępność, rozliczalność, autentyczność, niezaprzeczalność i niezawodność przetwarzanych danych osobowych .....</i>	<i>8</i>
<i>Rozdział 7. Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe .....</i>	<i>9</i>
Wykaz załączników .....	10

## Stosowane definicje

**Administrator danych osobowych**, zwany dalej „ADO” – organ, jednostka organizacyjna, podmiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych. W Kuratorium Oświaty w Warszawie zadania Administratora danych osobowych wykonuje Mazowiecki Kurator Oświaty.

**Administrator bezpieczeństwa informacji**, zwany dalej „ABI” – osoba wyznaczona przez ADO, pełniąca obowiązki wskazane w art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926, z późn. zm.), zwanej dalej „ustawą” i odpowiedzialna za nadzór nad zapewnieniem bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym Kuratorium Oświaty w Warszawie.

**Administrator systemu informatycznego**, zwany dalej „ASI” – osoba wyznaczona przez ADO, odpowiedzialna za nadzór nad zapewnieniem poprawnego i bezpiecznego przetwarzania informacji w systemie informatycznym Kuratorium Oświaty w Warszawie oraz za sprawność, konserwację i wdrażanie technicznych zabezpieczeń tego systemu przez lokalnych administratorów systemu.

**Lokalni administratorzy systemu**, zwani dalej „LAS” – osoby podlegające ASI, odpowiedzialne w Kuratorium i w delegaturach za praktyczną realizację zadań dotyczących zapewnienia poprawnego i bezpiecznego przetwarzania informacji w systemie informatycznym oraz za sprawność, konserwację i wdrażanie technicznych zabezpieczeń tego systemu.

**Osoba upoważniona do przetwarzania danych osobowych**, zwana dalej „osobą upoważnioną” – osoba, której ADO nadał uprawnienia w formie pisemnego upoważnienia do przetwarzania danych osobowych w określonym czasie i zakresie i dla której upoważnienie to nie zostało całkowicie wycofane.

**Przetwarzanie danych osobowych** – rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemie informatycznym.

**System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych.

**Użytkownik systemu informatycznego**, zwany dalej „użytkownikiem” – pracownik korzystający z systemu informatycznego Kuratorium Oświaty w Warszawie przy wykonywaniu powierzonych obowiązków służbowych.

**Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

**Stacja robocza** – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie.

## **Część 1. Cel i zakres polityki bezpieczeństwa**

1. Niniejsza polityka bezpieczeństwa określa podstawowe zasady bezpiecznego przetwarzania danych osobowych w Kuratorium.
2. Polityka bezpieczeństwa stanowi podstawę dla określenia szczegółowych zasad przetwarzania danych osobowych w Kuratorium.
3. Polityka bezpieczeństwa obejmuje swoim zakresem zbiory danych osobowych przetwarzanych w Kuratorium, zarówno w formie elektronicznej jak i papierowej.

## **Część 2. Deklaracja Administratora danych osobowych**

1. ADO, mając na względzie zapewnienie ochrony przetwarzanych danych osobowych zgodnie z wymaganiami prawnymi, deklaruje wsparcie dla działań i inicjatyw mających na celu właściwe zabezpieczenie przetwarzanych danych osobowych.
2. ADO w szczególności deklaruje zapewnienie alokacji zasobów na potrzeby zabezpieczenia przetwarzania danych osobowych, gdy jest to niezbędne ze względu na spełnienie obowiązujących wymagań prawnych, a także, gdy jest to uzasadnione żywotnymi interesami Kuratorium.

## **Część 3. Podstawowe zasady ochrony danych osobowych**

1. Przetwarzanie danych osobowych odbywa się w sposób zapewniający zgodność z wymaganiami ustawy oraz wydanych na jej podstawie aktów wykonawczych.
2. Kuratorium zapewnia ochronę przetwarzanych danych osobowych w zakresie wymaganym przepisami prawnymi oraz zgodnym z dobrymi praktykami.
3. Ochrona przetwarzanych danych osobowych obejmuje zapewnienie zabezpieczenia poufności, integralności, dostępności i rozliczalności, przy czym przez:
  - 1) **poufność** rozumie się zapewnienie, że dane nie będą udostępniane lub ujawniane nieautoryzowanym i nieupoważnionym osobom, podmiotom lub procesom;
  - 2) **integralność** rozumie się zapewnienie, że dane nie będą zmienione lub zniszczone w sposób nieautoryzowany;
  - 3) **dostępność** rozumie się zapewnienie, że osoby upoważnione do przetwarzania danych osobowych będą miały do nich dostęp w czasie wymaganym w związku z realizacją zadań Kuratorium;
  - 4) **rozliczalność** rozumie się zapewnienie, że działania osoby upoważnionej do przetwarzania danych osobowych będą przypisane w sposób jednoznaczny tylko tej osobie.
4. Osoby upoważnione do przetwarzania danych osobowych są odpowiedzialne za zapewnienie bezpieczeństwa przetwarzanych danych osobowych, w zakresie określonym w upoważnieniu. ADO podejmuje działania w celu zapewnienia osobom upoważnionym odpowiedniego poziomu wiedzy w zakresie obowiązujących wymagań w obszarze bezpieczeństwa danych osobowych.

5. ADO wyznacza ABI i ASI. ABI odpowiada za koordynowanie i nadzorowanie przestrzegania zasad ochrony przetwarzania danych osobowych i bezpieczeństwa systemu informatycznego przetwarzającego te dane w Kuratorium. ASI nadzoruje zapewnienie poprawnego i bezpiecznego pod względem technicznym przetwarzania informacji w systemie informatycznym Kuratorium oraz jego funkcjonowanie, sprawność, konserwację i wdrażanie technicznych zabezpieczeń przez LAS.
6. ABI i ASI na podstawie informacji od LAS i użytkowników, nadzorują występowanie ryzyka, będącego zagrożeniem dla bezpieczeństwa przetwarzanych danych osobowych oraz system informatyczny przetwarzający te dane, dokonując jego analizy i szacowania oraz podejmują stosowne działania do jego likwidacji lub minimalizacji.
7. ABI informuje ADO o wzroście występowania ryzyka dla bezpieczeństwa przetwarzanych danych osobowych lub systemu informatycznego przetwarzającego te dane, podając informację o podjętych działaniach.
8. ABI sprawuje stały nadzór nad ochroną danych osobowych oraz ich przetwarzaniem, a zwłaszcza kontroluje dostęp do danych osobowych, systemu informatycznego przetwarzającego te dane oraz prawidłowością przetwarzania przez osoby upoważnione. ASI za pośrednictwem LAS sprawuje stały nadzór w powyższym zakresie pod kątem technicznym.
10. ADO nadaje uprawnienia do dostępu do danych osobowych i ich przetwarzania. Nadawanie uprawnień odbywa się poprzez wystawienie i wydanie w formie pisemnej stosownego upoważnienia do dostępu do danych osobowych i ich przetwarzania, zgodnie z „Procedurą nadawania uprawnień do przetwarzania danych osobowych i rejestrowania ich w systemie informatycznym w Kuratorium Oświaty w Warszawie” (**załącznik nr 1**).
11. Upoważnienia wystawiane i wydawane są osobom wyłącznie w zakresie niezbędnym do wykonywanych przez nich obowiązków służbowych. Podmioty zewnętrzne i osoby będące ich pracownikami mogą mieć wystawione i wydane upoważnienia do dostępu do danych osobowych i przetwarzania tych danych, pod warunkiem spełnienia wymagań formalnych i prawnych, tylko w zakresie uzasadnionym usługami świadczonymi na rzecz Kuratorium, przy jednoczesnym zapewnieniu ochrony danych osobowych.
12. Każda osoba upoważniona, z chwilą wystawienia dla niej upoważnienia i dopuszczenia jej do przetwarzania danych osobowych, jest wpisywana do „Ewidencji osób upoważnionych do przetwarzania danych osobowych w Kuratorium Oświaty w Warszawie” (**załącznik nr 4**) prowadzonej przez ABI.
13. Każde wystawione upoważnienie podlega wpisaniu w prowadzonej przez ABI „Ewidencji wydanych upoważnień do przetwarzania danych osobowych w Kuratorium Oświaty w Warszawie” (**załącznik nr 5**).
14. Każda osoba upoważniona przed wydaniem jej upoważnienia i dopuszczeniem do przetwarzania danych osobowych, potwierdza zapoznanie się z przepisami dotyczącymi ochrony danych osobowych oraz wybranymi problemami Polityki bezpieczeństwa danych osobowych w Kuratorium Oświaty w Warszawie i Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Kuratorium Oświaty w Warszawie, poprzez złożenie podpisu na „Liście oświadczeń osób upoważnionych o zapoznaniu się

z przepisami dotyczącymi ochrony danych osobowych w Kuratorium Oświaty w Warszawie" (**załącznik nr 6**), którą prowadzi ABI.

15. ABI i ASI podejmują i realizują działania związane z zapobieżeniem naruszeń bezpieczeństwa przetwarzanych danych osobowych i próbami nielegalnego dostępu osób nieupoważnionych do systemu informatycznego oraz do danych osobowych przetwarzanych w systemie informatycznym.
16. W przypadku wystąpienia incydentów i zdarzeń w zakresie naruszenia bezpieczeństwa przetwarzanych danych osobowych, ABI i ASI podejmują działania związane z likwidacją lub minimalizacją ich negatywnych skutków, określeniem i wykryciem przyczyn ich wystąpienia, wyciągnięciem konsekwencji służbowych wobec ewentualnych sprawców, a także podjęciem stosownych środków przeciwdziałających wystąpieniu podobnych incydentów lub zdarzeń w przyszłości. Jednym z takich środków jest odebranie lub czasowe zawieszenie uprawnień, realizowane poprzez odwołanie upoważnienia do przetwarzania danych osobowych.
17. Dane osobowe są przetwarzane w sposób zapewniający minimalne ryzyko utraty ich dostępności i związanych z tym negatywnych konsekwencji dla Kuratorium. Zadanie to realizowane jest poprzez zgodne z Instrukcją kancelaryjną, zarządzanie dokumentami oraz zapewnienie właściwej konfiguracji systemu informatycznego i zarządzania kopiami zapasowymi zbiorów danych osobowych zawartych w Instrukcji zarządzania systemem informatycznych.
18. Rażąco lub systematyczne naruszanie wymagań w zakresie zapewnienia bezpieczeństwa przetwarzanych danych osobowych w systemie informatycznym, zobowiązuje ASI do zablokowania tej osobie dostępu do systemu informatycznego i przetwarzanych w nim danych osobowych oraz złożenia za pośrednictwem ABI pisemnego wniosku do ADO o odebranie lub czasowe zawieszenie uprawnień do przetwarzania danych osobowych.
19. W przypadku konieczności udostępnienia podmiotom zewnętrznym danych osobowych podlegających ochronie dyrektorzy wydziałów/delegatur występują z pismem do ADO, w którym przedstawiają:
  - 1) jakie dane osobowe będą przekazywane,
  - 2) jakiemu podmiotowi zewnętrznemu będą przekazywane dane i w jakim celu,
  - 3) sposób przekazania tych danych w postaci zaszyfrowanej i hasłem podanym niezależnym kanałem komunikacyjnym,
  - 4) ASI udziela niezbędnych informacji co do technicznych możliwości realizacji przekazania informacji we wskazany sposób,a następnie po zaopiniowaniu pisma przez ABI, ADO zezwala na ich udostępnienie.
20. Szczegółowe wymagania i zasady bezpiecznego przetwarzania danych osobowych oraz funkcjonowania systemu informatycznego są określone w Instrukcji zarządzania systemem informatycznym w Kuratorium Oświaty w Warszawie. Nieprzestrzeganie obowiązujących wymagań i zasad ochrony przetwarzania danych osobowych i bezpieczeństwa systemu informatycznego może skutkować konsekwencjami służbowymi lub odpowiedzialnością cywilną lub karną przewidzianą prawem.
21. Polityka bezpieczeństwa danych osobowych w Kuratorium Oświaty w Warszawie i związane z nią dokumenty wykonawcze podlegają przeglądowi i aktualizacji przez ABI we współpracy z ASI raz na rok, lub na bieżąco w przypadku

wystąpienia zmian w przepisach prawnych i wprowadzeniu zmian organizacyjnych w Kuratorium.

## **Część 4. Sposób przetwarzania danych osobowych**

### **Rozdział 1. Obszar przetwarzania danych osobowych**

1. Dane osobowe przetwarzane są w siedzibie Kuratorium Oświaty w budynku przy Al. Jerozolimskich 32 i 28 w Warszawie oraz delegaturach w:
  - 1) Ciechanowie przy ul. Księdza Piotra Ściegiennego 9;
  - 2) Ostrołęce przy ul. Gorbatowa 15;
  - 3) Płocku przy ul. Kościuszki 20;
  - 4) Radomiu przy ul. Żeromskiego 53;
  - 5) Siedlcach przy ul. Piłsudskiego 38.
2. Zbiory danych osobowych w powyższych lokalizacjach, są przetwarzane w pomieszczeniach Kuratorium i delegatur wymienionych w **załączniku nr 7**.

### **Rozdział 2. Wykaz zbiorów danych osobowych i programów wykorzystywanych do przetwarzania danych osobowych**

Wykaz zbiorów danych osobowych i programów wykorzystywanych do przetwarzania danych osobowych w Kuratorium zawarty jest zgodnie ze wzorem w **załączniku nr 8**.

### **Rozdział 3. Poziom bezpieczeństwa przetwarzania danych osobowych**

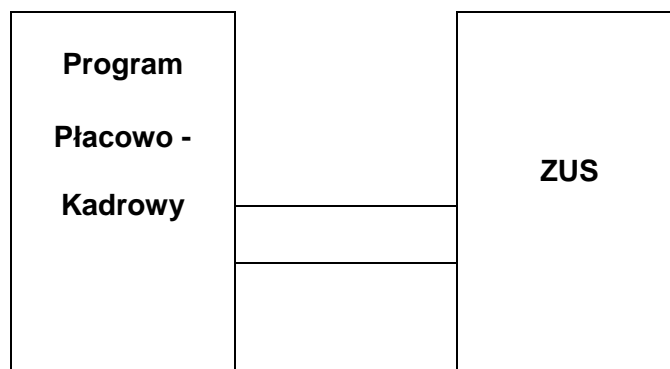
1. W odniesieniu do zbiorów danych osobowych przetwarzanych w systemie informatycznym stosuje się poziom wysoki.
2. Zbiory przetwarzane w formie papierowej muszą być zabezpieczone przed nieautoryzowanym dostępem, zabraniem, ujawnieniem czy zniszczeniem i stosuje się środki ochrony na poziomie podstawowym.

### **Rozdział 4. Opis struktury zbiorów danych osobowych**

Opisy struktur poszczególnych zbiorów danych osobowych przetwarzanych w Kuratorium przedstawione są zgodnie ze wzorem w **załączniku nr 9**.

### **Rozdział 5. Sposób przepływu danych pomiędzy poszczególnymi systemami**

Na poniższym schemacie przedstawiono istniejące przepływy danych pomiędzy systemami informatycznymi, wykorzystywanymi do przetwarzania danych osobowych.



### **Opis przepływów:**

Przepływ danych - dane przesyłane są z programu płacowo-kadrowego do ZUS.

### **Rozdział 6. Środki zapewniające poufność, integralność, dostępność i rozliczalność przetwarzanych danych osobowych**

1. Mechanizmy ochrony organizacyjnej:
  - 1) powołanie przez ADO ABI i ASI;
  - 2) wdrożenie Polityki bezpieczeństwa danych osobowych i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz załączników;
  - 3) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
  - 4) monitorowanie pracy infrastruktury informatycznej;
  - 5) badanie bezpieczeństwa infrastruktury informatycznej.
2. Mechanizmy ochrony logicznej:
  - 1) mechanizmy identyfikacji, uwierzytelnienia i kontroli dostępu na poziomie systemów operacyjnych i aplikacji;
  - 2) ograniczone uprawnienia użytkowników w systemach operacyjnych stacji roboczych;
  - 3) dostęp do internetu, stosownie do posiadanych środków technicznych, poprzez urządzenie programowe lub sprzętowe separujące sieć lokalną od sieci publicznej;
  - 4) narzędzia do bezpiecznego usuwania danych w miarę posiadanych możliwości sprzętowych;
  - 5) mechanizmy rozliczalności wprowadzenia i udostępnienia danych osobowych w programach, o ile jest to możliwe pod względem technicznym.
3. Mechanizmy ochrony fizycznej:
  - 1) ochrona obiektu, w tym zarządzanie kluczami do pomieszczeń oraz system kontroli dostępu do obiektu Kuratorium i delegatur;
  - 2) gaśnica do gaszenia urządzeń elektronicznych w serwerowni;
  - 3) system zasilania awaryjnego (UPS) przy serwerach;
  - 4) kontrola dostępu do serwerowni.



## Rozdział 7. Zasady korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe

1. Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków. Przetwarzanie danych osobowych przy użyciu komputerów przenośnych może odbywać się wyłącznie za zgodą ADO i za wiedzą ABI i ASI.
2. Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza na dostęp do nich osób nieupoważnionych. Użytkownik komputera przenośnego zobowiązany jest do:
  - 1) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia;
  - 2) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego;
  - 3) niezezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe;
  - 4) zabezpieczania komputera przenośnego hasłem;
  - 5) blokowania dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez pracownika;
  - 6) umożliwienia, poprzez podłączenie komputera do sieci informatycznej KO lub Internetu, aktualizacji wzorców wirusów w programie antywirusowym;
  - 7) utrzymania konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z hasła;
  - 8) wykorzystywania hasła zgodnych z wytycznymi dotyczącymi tworzenia hasła w systemie informatycznym przetwarzającym dane osobowe.
3. ABI i ASI zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, aby:
  - 1) dokonano konfiguracji oprogramowania w sposób wymuszający korzystanie z hasła, wykorzystywanie hasła zgodnych z wytycznymi dotyczącymi tworzenia hasła w systemie informatycznym przetwarzającym dane osobowe oraz wymuszającym okresową ich zmianę, o ile jest to możliwe pod względem technicznym;
  - 2) zbiory danych osobowych były przechowywane w komputerach przenośnych w postaci zaszyfrowanej, gwarantującej dostęp wyłącznie upoważnionemu użytkownikowi, o ile jest to możliwe technicznie;
  - 3) dokonano instalacji i konfiguracji oprogramowania antywirusowego na komputerze przenośnym oraz aktualizacji wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.
4. ABI jest odpowiedzialny za prowadzenie ewidencji komputerów przenośnych wykorzystywanych do przetwarzania danych osobowych, która obejmuje:
  - 1) numer ewidencyjny i seryjny komputera przenośnego;
  - 2) imię i nazwisko osoby będącej użytkownikiem komputera;
  - 3) zbiór danych osobowych przetwarzanych na komputerze przenośnym.
5. W razie zagubienia lub kradzieży pracownik zobowiązany jest do natychmiastowego powiadomienia ABI i ASI zgodnie z zasadami informowania o naruszeniu ochrony danych osobowych.

### **Wykaz załączników**

**Załącznik Nr 1** Procedura nadawania uprawnień do przetwarzania danych osobowych i rejestrowania ich w systemie informatycznym Kuratorium Oświaty w Warszawie.

**Załącznik Nr 2** Wniosek w sprawie wystawienia i wydania upoważnienia do przetwarzania danych osobowych w Kuratorium Oświaty w Warszawie.

**Załącznik Nr 3** Upoważnienie do przetwarzania danych osobowych w Kuratorium Oświaty w Warszawie.

**Załącznik Nr 4** Ewidencja osób upoważnionych do przetwarzania danych osobowych w Kuratorium Oświaty w Warszawie.

**Załącznik Nr 5** Ewidencja wydanych upoważnień do przetwarzania danych osobowych w Kuratorium Oświaty w Warszawie.

**Załącznik Nr 6** Lista oświadczeń osób upoważnionych o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych w Kuratorium Oświaty w Warszawie.

**Załącznik Nr 7** Wykaz pomieszczeń w Kuratorium Oświaty w Warszawie i delegaturach, w których przechowywane i przetwarzane są zbiory danych osobowych.

**Załącznik Nr 8** Wykaz zbiorów danych osobowych i programów wykorzystywanych do przetwarzania danych osobowych w Kuratorium Oświaty w Warszawie.

**Załącznik Nr 9** Opis struktury zbiorów danych osobowych.

Załącznik Nr 1  
do Polityki bezpieczeństwa danych osobowych  
w Kuratorium Oświaty w Warszawie

## **PROCEDURA**

**nadawania uprawnień do przetwarzania  
danych osobowych i rejestrowania ich  
w systemie informatycznym  
w Kuratorium Oświaty w Warszawie**

1. Nadanie uprawnień do przetwarzania danych osobowych osobie będącej pracownikiem Kuratorium, następuje na podstawie złożonego przez jego kierownika komórki organizacyjnej, pisemnego wniosku (**załącznik nr 2**) do Administratora danych osobowych (ADO) o wystawienie i wydanie imiennego upoważnienia.
2. Nadanie uprawnień do przetwarzania danych osobowych osobie będącej pracownikiem podmiotu zewnętrznego, któremu powierzono przetwarzanie danych osobowych w systemie informatycznym Kuratorium, następuje na podstawie złożonego przez kierownika tego podmiotu, pisemnego wniosku (**załącznik nr 2**) do ADO o wystawienie i wydanie imiennego upoważnienia.
3. ADO przed wystawieniem i wydaniem upoważnienia, przekazuje otrzymany wniosek Administratorowi bezpieczeństwa informacji (ABI) w celu dokonania jego weryfikacji pod względem formalnym.
4. Niespełnianie wymagań formalnych skutkuje odesłaniem wniosku przez ABI do wnioskodawcy z prośbą o jego uzupełnienie i ponowne złożenie do ADO.
5. W przypadku braku uwag do przedłożonego wniosku i zastrzeżeń wobec wskazanej w nim osoby, ABI wystawia (w trzech egzemplarzach) pisemne imienne „Upoważnienie do przetwarzania danych osobowych w Kuratorium Oświaty w Warszawie” dla wskazanej we wniosku osoby (**załącznik nr 3**).
6. Wystawione imienne upoważnienie ABI przedkłada ADO do akceptacji i podpisu.
7. Po podpisaniu przez ADO, każde wystawione upoważnienie podlega zarejestrowaniu w prowadzonej przez ABI „Ewidencji wydanych upoważnień do przetwarzania danych osobowych w Kuratorium Oświaty w Warszawie” (**załącznik nr 5**).
8. Podpisane przez ADO upoważnienie ABI przedstawia osobie, dla której zostało wystawione celem zapoznania z jego treścią i podpisania każdego z trzech egzemplarzy, a następnie:
  - 1) jeden egzemplarz wydaje osobie upoważnionej;
  - 2) drugi egzemplarz przekazuje do teczki akt osobowych pracownika;
  - 3) trzeci egzemplarz przechowywany jest przez ABI w teczce wydanych upoważnień.
9. ABI zapoznaje osobę z przepisami dotyczącymi ochrony danych osobowych obowiązującymi w Kuratorium i dokonuje odpowiedniego wpisu w „Liście oświadczeń osób upoważnionych o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych w Kuratorium” (**załącznik nr 6**).
10. W przypadku osób będących pracownikami podmiotów zewnętrznych, wszystkie egzemplarze upoważnienia są przekazywane upoważnionemu przedstawicielowi tego podmiotu. Po zapoznaniu się z treścią i podpisaniu każdego egzemplarza przez osobę, dla której zostało wystawione, jeden egzemplarz jest zwracany ABI i przechowywany przez niego w teczce wydanych upoważnień.
11. Administrator systemu informatycznego (ASI) na pisemny wniosek ABI zleca właściwemu Lokalnemu Administratorowi Systemu (LAS) nadanie uprawnień do pracy w systemie informatycznym, który dokonuje rejestracji uprawnień w systemie. W przypadku nadawania uprawnień po raz pierwszy, LAS dokonuje wygenerowania identyfikatora użytkownika i wygenerowania hasła tymczasowego. LAS przekazuje osobie upoważnionej identyfikator i hasło. Upoważniona osoba jest zobowiązana do zmiany otrzymanego hasła przy pierwszym logowaniu się do systemu informatycznego.

12. ABI na podstawie zwrotnej informacji od ASI, niezwłocznie dokonuje odpowiednich wpisów w „Ewidencji osób upoważnionych do przetwarzania danych osobowych w Kuratorium Oświaty w Warszawie ” (**załączniku nr 4**).
13. Zarządzanie uprawnieniami do przetwarzania danych osobowych w systemie informatycznym musi być zgodne z zasadą minimalnych uprawnień oraz zasadą wiedzy koniecznej i uzasadnionej.
14. Złożone do ADO wnioski o nadanie uprawnień do przetwarzania danych osobowych przechowuje ABI.

Załącznik Nr 2

do Polityki bezpieczeństwa danych osobowych w Kuratorium Oświaty w Warszawie

...../.....

Miejscowość, data

**Imię i nazwisko**  
**Administrator danych osobowych w KO**  
**w miejscu**

## W N I O S E K

**w sprawie wystawienia i wydania upoważnienia do przetwarzania  
danych osobowych w Kuratorium Oświaty w Warszawie**

W związku z realizacją .....,  
(nazwa programu/zadania)  
proszę o nadanie uprawnień do dostępu i przetwarzania danych osobowych  
w zbiorze danych .....,  
(nazwa zbioru)  
poprzez wystawienie i wydanie upoważnienia dla Pana/Pani  
....., w zakresie  
(imię i nazwisko)  
..... z terminem ważności  
(wykonywane czynności )  
od dnia ..... do dnia .....

Dyrektor *(lub osoba upoważniona)*

do Polityki bezpieczeństwa danych osobowych w Kuratorium Oświaty w Warszawie

## **KURATORIUM OŚWIATY W WARSZAWIE**

### **ADMINISTRATOR DANYCH OSOBOWYCH**

Warszawa, dnia.....

### **UPOWAŻNIENIE Nr ...../ABI/20.....**

#### **do przetwarzania danych osobowych w Kuratorium Oświaty w Warszawie**

W związku z art.37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.02.101.926 z późn. zm.) upoważniam Panią/Pana .....  
do przetwarzania danych osobowych zawartych w zbiorze .....  
w zakresie niezbędnym do realizacji zadań.

Niniejsze upoważnienie jest ważne od dnia ..... do dnia .....

.....  
Podpis Administratora danych osobowych

Zgodnie z art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) zobowiązuję się do zachowania w tajemnicy treści przetwarzanych danych osobowych, zarówno podczas wykonywania powierzonych zadań, jak i po zaprzestaniu ich wykonywania.

Jednocześnie oświadczam, że zapoznałem się z zasadami ochrony danych osobowych i obowiązuję się do ich przestrzegania.

.....  
Data i podpis osoby upoważnionej

Sporządzono w 3 egz.:

- 1.Osoba upoważniona
- 2.Teczka akt osobowych pracownika
- 3.ABI

do Polityki bezpieczeństwa danych osobowych w Kuratorium Oświaty w Warszawie

**Ewidencja****osób upoważnionych do przetwarzania danych osobowych w Kuratorium Oświaty**

Lp.	Imię i nazwisko	Identyfikator użytkownika	Zakres przydzielonych uprawnień	Data przyznania uprawnień	Podpis ABI	Data odebrania uprawnień	Podpis ABI

do Polityki bezpieczeństwa danych osobowych w Kuratorium Oświaty w Warszawie

**Ewidencja****wydanych upoważnień do przetwarzania danych osobowych w Kuratorium Oświaty**

Numer upoważnienia	Komórka organizacyjna	Nazwisko	Imię	Identyfikator użytkownika	Zakres przydzielonych uprawnień	Data	
						przyznania uprawnień	odebrania uprawnień

do Polityki bezpieczeństwa danych osobowych w Kuratorium Oświaty w Warszawie

**Lista****oświadczeń osób upoważnionych o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych w Kuratorium Oświaty w Warszawie****Oświadczam, że zapoznałem(am) się z:**

- przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz przepisami wykonawczymi do niniejszej ustawy;
- Polityką bezpieczeństwa danych osobowych w Kuratorium Oświaty w Warszawie;
- Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Kuratorium Oświaty w Warszawie.

L.p.	Imię i nazwisko	Data	Podpis osoby upoważnionej potwierdzający zapoznanie się z ww. dokumentami

Załącznik Nr 7

do Polityki bezpieczeństwa danych osobowych w Kuratorium Oświaty w Warszawie

**Wykaz**  
**pomieszczeń Kuratorium Oświaty w Warszawie i delegatur,**  
**w których przechowywane i przetwarzane są zbiory danych osobowych**

Numer pomieszczenia	Zbiór danych osobowych przechowywanych i przetwarzanych w pomieszczeniu

Załącznik Nr 8

do Polityki bezpieczeństwa danych osobowych w Kuratorium Oświaty w Warszawie

**Wykaz**  
**zbiorów danych osobowych i programów wykorzystywanych do przetwarzania danych**  
**osobowych w Kuratorium Oświaty w Warszawie**

L.p.	Nazwa zbioru danych osobowych	Nazwa programu

Załącznik nr 9

do Polityki bezpieczeństwa danych osobowych w Kuratorium Oświaty w Warszawie

**Opis struktury zbiorów danych osobowych**

Nazwa zbioru danych osobowych

L.p.	Nazwa pola/Rodzaj informacji	Opis lub uwagi