

ZARZĄDZENIE Nr 2/2017

Dyrektora CENTRUM USŁUG WSPÓLNYCH W OKONKU

z dnia 02.01.2017 r.

w sprawie: wprowadzenia Polityki bezpieczeństwa i Instrukcji Zarządzania Systemem Przetwarzania Danych Osobowych.

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922 z późn. zm.) oraz § 3 i 4 rozporządzenia 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).

Zarządza się, co następuje:

§ 1

Wprowadzam w **CENTRUM USŁUG WSPÓLNYCH W OKONKU** Politykę Bezpieczeństwa, której treść stanowi załącznik nr 1 do zarządzenia oraz Instrukcję Zarządzania systemem przetwarzania danych osobowych przy użyciu systemu informatycznego i w sposób ręczny, która stanowi załącznik nr 2 do zarządzenia.

§ 2

Każdy pracownik, zgodnie z wykazem, jest obowiązany zapoznać się z treścią załącznika nr 1 i nr 2 do zarządzenia.

§ 3

Wyznacza się Panią Katarzynę Kot- inspektora ds. księgowości na Administratora Bezpieczeństwa Informacji w Centrum Usług Wspólnych w Okonku

§ 4

Dyrektor placówki zobowiązuje wszystkich pracowników do przestrzegania Polityki Bezpieczeństwa oraz stosowania w pracy Instrukcji pod groźbą konsekwencji służbowych, przewidzianych prawem.

DYREKTOR
Centrum Usług Wspólnych
w Okonku
Renata Zabrocka

POLITYKA BEZPIECZEŃSTWA

Administrator Danych **RENATA ZABROCKA**

Dnia 02.01.2017 r. w podmiocie o nazwie **CENTRUM USŁUG WSPÓLNYCH W OKONKU**

Zgodnie z **ROZPORZĄDZENIEM 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)
wdraża dokument o nazwie „Polityka Bezpieczeństwa”. Zapisy tego dokumentu wchodzi w życie z dniem 02.01.2017 r.

§ 1.

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w **CENTRUM USŁUG WSPÓLNYCH W OKONKU**, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych.

§ 2

Ilekroć w „Polityce Bezpieczeństwa” jest mowa o:

1. zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. przetwarzaniu danych - 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 systemach informatycznych,
3. systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
5. usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6. administratorze danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych,

7. administratorze bezpieczeństwa informacji – rozumie się przez to osobę wyznaczoną przez Administratora Danych w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w ust. 1, chyba, że Administrator Danych sam wykonuje te czynności.
8. podmiocie – rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;

§ 3.

Administrator Danych wyznacza **Administratora Bezpieczeństwa Informacji** w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Upoważnienie dla **Administratora Bezpieczeństwa Informacji** oraz zakres obowiązków określa załącznik do „Polityki Bezpieczeństwa” nr 1.

§ 4.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa załącznik do „Polityki Bezpieczeństwa” nr 2.

§ 5.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych określa załącznik do „Polityki Bezpieczeństwa” nr 3.

§ 6.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami określa załącznik do „Polityki Bezpieczeństwa” nr 4.

§ 7.

W podmiocie dokłada się wszelkich starań, aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty znajdują się w pomieszczeniu zamkniętym na klucz, do którego dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych.

§ 8.

Do przetwarzania danych dopuszczone są wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych**. **Administrator Danych** stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator Danych nadaje uprawnienia pracownikom, którzy przetwarzają dane poprzez podpisanie upoważnienia, które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa”**. Prowadzona jest dokumentacja opisująca sposób przetwarzania danych w podmiocie, a w szczególności:

1. Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie – **załącznik nr 6 do „Polityki Bezpieczeństwa”**.
2. Zestawienie danych osobowych. Kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane – **załącznik nr 7 do „Polityki Bezpieczeństwa”**.
3. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych - **załącznik nr 8 do „Polityki Bezpieczeństwa”**.

§ 9.

Na wniosek osoby, której dane dotyczą, Administrator Danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji.

§ 10.

Administrator Danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych osobowych w podmiocie. Podmiot ten może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

§ 11.

Sposób zabezpieczenia oraz przetwarzania danych w systemie informatycznym reguluje Instrukcja Zarządzania Systemem Informatycznym.

§ 12.

W sprawach nieuregulowanych w niniejszej „Polityce Bezpieczeństwa” mają zastosowanie odpowiednie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **ROZPORZĄDZENIA 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**

§ 13.

Deklaracja intencji, cele i zakres polityki bezpieczeństwa

1. Administrator Danych wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.
2. Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów, w których dochodzi do przetwarzania danych osobowych.
3. Polityka dotyczy wszystkich danych osobowych przetwarzanych w podmiocie, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.
4. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych w tym oddziałów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych.

Celem Polityki jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy

- a) poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
- b) integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- c) rozliczalności - właściwości zapewniającej, że działania podmiotu operującego na danych osobowych mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- d) ciągłości - zdolności do niezakłóconego ich przetwarzania, bez przerw uniemożliwiających ich udostępnianie osobom upoważnionym.

8. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:

- a) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne;
- b) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;
- c) kontrolę i nadzór nad przetwarzaniem danych osobowych;
- d) monitorowanie zastosowanych środków ochrony;
- e) ciągłe śledzenie zmieniających się zagrożeń wewnętrznych i zewnętrznych, także uwzględnianie zmieniającego się prawa;
- f) kontrolę i nadzór nad przetwarzaniem danych osobowych przez podmioty trzecie, którym dane zostały udostępnione lub powierzone.

9. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.

10. Administrator Danych lub osoba przez niego upoważniona wdraża wszystkie niezbędne dokumenty wynikające z zapisów ustawy oraz innych przepisów mających zastosowania przy przetwarzaniu danych osobowych.

Administrator Bezpieczeństwa Informacji

INSPEKTOR
ds. księgowości budżetowej

Katarzyna Kot

Administrator Danych

DYREKTOR
Centrum Usług Wspólnych
w Okonku

Renata Zabrocka

Administrator Danych **RENATA ZABROCKA**

Dnia 02.01.2017 r. w podmiocie o nazwie **CENTRUM USŁUG WSPÓLNYCH W OKONKU**

Zgodnie z **ROZPORZĄDZENIEM 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
wdraża dokument o nazwie „Instrukcja zarządzania systemem informatycznym” zwany dalej „instrukcją”. Zapisy tego dokumentu wchodzi w życie z dniem **02.01.2017 r.**

Ilekcroć w „instrukcji” jest mowa o:

- 1) podmiocie — rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nie posiadający osobowości prawnej, jednostkę budżetową;
- 2) ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą”;
- 3) identyfikatorze użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- 4) haśle — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- 5) sieci telekomunikacyjnej — rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. z 2016, poz. 1489, z późn. zm.)
- 6) sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
- 7) teletransmisji — rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej
- 8) rozliczalności — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- 9) integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- 10) raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
- 11) poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
- 12) uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 1

Za przestrzeganie w podmiocie **CENTRUM USŁUG WSPÓLNYCH W OKONKU** zapisów „Instrukcji” odpowiedzialny jest Administrator danych lub zgodnie z zapisem §2 „Polityki Bezpieczeństwa” wyznaczony **Administrator Bezpieczeństwa Informacji**.

§2

W związku z tym, że w podmiocie **CENTRUM USŁUG WSPÓLNYCH W OKONKU** przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie **wysokim**, a w związku z tym wprowadza się poniższe postanowienia:

I

Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora Danych, Administratora Bezpieczeństwa Informacji lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

II

1. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora Bezpieczeństwa Informacji. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się

z co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:

w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

•poprzez zainstalowanie programu antywirusowego o nazwie **GData Internet Security**

•poprzez zainstalowanie firewall (zapora sieciowa).

IV

1. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być

przydzielony innej osobie.

2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz w miesiącu.
4. Kopie zapasowe:
 - a) przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym

ARCHIWUM

zaopatrzone w drzwi zamykane na klucz, alarm

- b) usuwane niezwłocznie po ustaniu ich użyteczności.

V

Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.

VI

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- 1) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- 2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- 3) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§3

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:

- 1) daty pierwszego wprowadzenia danych do systemu;
- 2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
- 3) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;
- 4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;

5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje,
o których mowa w ust. 1.

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§4

Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek wylogować się z systemu. W przypadku braku czynności ze strony użytkownika w systemie informatycznym przez 30 min, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.

§5

Administrator Bezpieczeństwa Informacji ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w podmiocie oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co 30 dni oraz przeglądów generalnych raz na rok. W przypadku stwierdzenia usterek technicznych **Administrator Bezpieczeństwa Informacji** ma obowiązek niezwłocznie powiadomić o tym fakcie Administratora Danych.

§6

W przypadku stwierdzenia przez **Administratora Bezpieczeństwa Informacji** uchybień dotyczących przetwarzania danych w podmiocie powinien o tym fakcie niezwłocznie powiadomić Administratora Danych oraz wprowadzić takie zabezpieczenia i procedury, które w przyszłości wyeliminują takie zdarzenia.

§ 7.

W sprawach nieuregulowanych w niniejszej „instrukcji” mają zastosowanie przepisy ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. oraz **ROZPORZĄDZENIEM 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

DYREKTOR
Centrum Usług Wspólnych
Podpis Administratora Danych Osobowych

.....
Renata Zabrocka

Podpis

Podpis Administratora Bezpieczeństwa Informacji

INSPEKTOR
ds. księgowości budżetowej
.....

Katarzyna Kot

Upoważnienie dla Administratora Bezpieczeństwa Informacji oraz zakres obowiązków

załącznik nr 1 do „Polityki Bezpieczeństwa”

Na podstawie § 3 Polityki Bezpieczeństwa z dnia 23.11.2016 r. zgodnie z założeniami
ROZPORZĄDZENIEM 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**

Na podstawie art. 36a ust. 1 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2016 r. poz. 922 z późn. zm.)

Administrator Danych RENATA ZABROCKA powołuje w podmiocie **CENTRUM USŁUG WSPÓLNYCH W OKONKU** NIP: 767-17-04-789

Administratora Bezpieczeństwa Informacji KATARZYŃĘ KOT

Pesel 84061405701

Upoważnienie jest ważne od chwili podpisania przez strony do dnia odwołania Administratora Bezpieczeństwa Informacji przez Administratora Danych Osobowych.

Zgodnie z art. 36a ust.2 **do zadań ABI należy:**

- 1) zapewnianie przestrzegania przepisów o ochronie danych osobowych,
- 2) prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7 zgodnie z zapisami Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (Dz. U. 2015 poz. 745).

Administrator Bezpieczeństwa Informacji nadzoruje opracowanie i aktualizowanie dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych. Jest odpowiedzialny za przestrzeganie w podmiocie zapisów Instrukcji Zarządzania Systemem Informatycznym. **Administrator Bezpieczeństwa Informacji** prowadzi wszelką dokumentację opisującą sposób przetwarzania danych w podmiocie, a w szczególności:

zgodnie z § 4. „Polityki Bezpieczeństwa”

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, który określa załącznik do „Polityki Bezpieczeństwa” nr 2,

zgodnie z § 5. „Polityki Bezpieczeństwa”

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych

do przetwarzania tych danych, który określa załącznik do „Polityki Bezpieczeństwa” nr 3,

zgodnie z § 6. „Polityki Bezpieczeństwa”

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, który określa załącznik do „Polityki Bezpieczeństwa” nr 4,

zgodnie z § 8. „Polityki Bezpieczeństwa”

Ewidencję osób przetwarzających dane w podmiocie posiadających upoważnienie - załącznik nr 6 do „Polityki Bezpieczeństwa” oraz zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane – załącznik nr 7 do „Polityki Bezpieczeństwa”.

Administrator Bezpieczeństwa Informacji sprawdza zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje w tym zakresie sprawozdania dla administratora danych lub na wniosek GIODO zgodnie z zapisami Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (Dz. U. 2015 poz. 745).

Administrator Bezpieczeństwa Informacji zapewnia zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Administrator danych zapewnia środki i organizacyjną odrębność Administratora Bezpieczeństwa Informacji niezbędne do należytego wykonywania przez niego zadań wynikających z niniejszego upoważnienia i przepisów ustawy.

OŚWIADCZENIE ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

Oświadczam, że zapoznałem się z treścią i obowiązkami wynikającymi z tego upoważnienia oraz, że jako administrator bezpieczeństwa informacji, będę nadzorował przestrzeganie zasad ochrony danych w podmiocie **CENTRUM USŁUG WSPÓLNYCH W OKONKU** zgodnie z obowiązkami wynikającymi z tego upoważnienia oraz ustawy o ochronie danych osobowych.

Oświadczam, że spełniam wymogi dotyczące osoby powołanej na stanowisko Administratora Bezpieczeństwa informacji tj.:

- nie byłem/byłem karana/y za umyślne przestępstwo,
- posiadam pełną zdolność do czynności prawnych oraz korzystam z pełni praw publicznych,
- posiadam odpowiednią wiedzę z zakresu ochrony danych osobowych.

Administrator Bezpieczeństwa Informacji

INSPEKTOR
ds. księgowości budżetowej

Katarzyna Kot

.....
.....

Administrator Danych

DYREKTOR
Centrum Usług Wspólnych
w Okonku

Renata Zabrocka

załącznik do „Polityki Bezpieczeństwa” nr 3 zgodnie, z § 4 pkt 2 Rozporządzenia Ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r.

Lp.	Nazwa zbioru danych <i>(np. dane klientów, pracowników itd.)</i>	Programy zastosowane do przetwarzania danych <i>(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)</i>	Uwagi
1	Akta osobowe pracowników Centrum Usług Wspólnych	Wersja papierowa	
2	Akta osobowe dyrektorów placówek podlegających pod CUW	Wersja papierowa	
3	Ewidencja czasu pracy	Wersja papierowa	
4	Ewidencja czasu pracy	Wersja elektroniczna	
5	Listy płac pracowników CUW oraz pracowników podlegających pod CUW	Wersja papierowa	
6	Listy płac pracowników CUW oraz pracowników podlegających pod CUW	Wersja elektroniczna	
7	Dane pracownicze do ubezpieczenia	Wersja papierowa	
8	Dane pracownicze do ubezpieczenia	Wersja elektroniczna	
9	Ubezpieczenia zbiorcze pracowników	Wersja papierowa	
10	Ubezpieczenia zbiorcze pracowników	Wersja elektroniczna	
11	Dokumentacja wypadkowa pracowników	Wersja papierowa	
12	Dokumentacja emerytalno rentowa, Rp-7	Wersja papierowa	
13	Dokumentacja związana z organizacją staży zawodowych, praktyk	Wersja papierowa	
14	Umowy cywilno prawne, prace zlecenia na rzecz szkoły	Wersja papierowa	
15	Zbiór danych do SIO	Wersja papierowa	
16	Zbiór danych do SIO	Wersja elektroniczna	
17	Obowiązek szkolny	Wersja papierowa	
18	Dotacje dla placówek niepublicznych	Wersja papierowa	
19	Dowody księgowe CUW oraz jednostek podlegających pod CUW	Wersja papierowa	

Lp.	Nazwa zbioru danych <i>(np. dane klientów, pracownikó w itd.)</i>	Programy zastosowane do przetwarzania danych <i>(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)</i>	Uwagi
20	Dowody księgowe CUW oraz jednostek podlegających pod CUW	Wersja elektroniczna	
21	Organizacja dowozu	Wersja papierowa	
22	Dokumentacja rozliczeniowa z ZUS -Płatnik	Wersja papierowa	
23	Dokumentacja rozliczeniowa z ZUS -Płatnik	Wersja elektroniczna	
24	Dziennik korespondencji	Wersja papierowa	
25	Dziennik korespondencji	Wersja elektroniczna	
26	Zalecenia pokontrolne	Wersja papierowa	
27	Wnioski o nagrody, medale, odznaczenia	Wersja papierowa	
28	Skierowania na badania	Wersja papierowa	
29	Sprawozdania z wykonania budżetu, plany finansowe	Wersja papierowa	
30	Sprawozdania z wykonania budżetu, plany finansowe	Wersja elektroniczna	
31	Dokumenty założycielskie jednostki	Wersja papierowa	
32	Ewidencja placówek niepublicznych	Wersja papierowa	
33	Inwentaryzacja	Wersja papierowa	
34	Bilans jednostek	Wersja papierowa	
35	Zaświadczenia o dochodach, zatrudnieniu CUW i jednostek podlegających pod CUW	Wersja papierowa	
36	Potrącenia z wynagrodzenia	Wersja papierowa	
37	Pracownicy młodociani	Wersja papierowa	
38	Pracownicy młodociani	Wersja elektroniczna	
39	Godziny ponadwymiarowe	Wersja papierowa	
40	Absencja w pracy, rejestr zwolnień lekarskich	Wersja papierowa	
41	Absencja w pracy, rejestr zwolnień lekarskich	Wersja elektroniczna	
42	Karty zasilkowe	Wersja papierowa	
43	Karty zasilkowe	Wersja elektroniczna	
44	Karty wynagrodzeń	Wersja papierowa	

Lp.	Nazwa zbioru danych <i>(np. dane klientów, pracowników itd.)</i>	Programy zastosowane do przetwarzania danych <i>(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)</i>	Uwagi
45	Karty wynagrodzeń	Wersja elektroniczna	
46	ZFŚS CUW	Wersja papierowa	
47	PIT-11, PIT-40	Wersja papierowa	
48	PIT-11, PIT-40	Wersja elektroniczna	
49	PIT-40A	Wersja papierowa	

Data i podpis Administratora Bezpieczeństwa Informacji

..... J. EKOR
as. księgowości budżetowej

Katarzyna Koi

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe złącznik do „Polityki Bezpieczeństwa” nr 2 zgodnie z § 4 pkt 1 Rozporządzenia Ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r.

Lp.	Dokładny adres <i>(np. adres siedziby firmy gdzie przetwarzane są dane)</i>	Dział użytkujący pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
1	CENTRUM USŁUG WSPÓLNYCH W OKONKU Ul. Leśna 46 64-965 Okonek	Gabinet dyrektora	Gabinet dyrektora	Alarm, drzwi zamknięte na klucz, monitoring zewnętrzny, szafy zamknięte na klucz	
2	CENTRUM USŁUG WSPÓLNYCH W OKONKU Ul. Leśna 46 64-965 Okonek	Dział placowy	Pokój pierwszy	Alarm, drzwi zamknięte na klucz, monitoring zewnętrzny, szafy zamknięte na klucz, szafy metalowe zamknięte na klucz	
4	CENTRUM USŁUG WSPÓLNYCH W OKONKU Ul. Leśna 46 64-965 Okonek	Dział księgowy	Pokój drugi	Alarm, drzwi zamknięte na klucz, szafy zamknięte na klucz, szafy pancerne	
5	CENTRUM USŁUG WSPÓLNYCH W OKONKU Ul. Leśna 46 64-965 Okonek	Dział księgowy	Pokój trzeci	Drzwi zamknięte na klucz, alarm, szafy zamknięte na klucz, szafy pancerne	
6	CENTRUM USŁUG WSPÓLNYCH W OKONKU Ul. Leśna 46 64-965 Okonek	Archiwum	Brak numeru	Drzwi zamknięte na klucz, alarm	

Data i podpis Administratora Danych Osobowych

INSPEKTOR

ds. księgowości budżetowej

Kuczyński

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych
- załącznik do „Polityki Bezpieczeństwa” nr 4 zgodnie, z § 4 pkt 3 i 4 Rozporządzenia Ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r.

Lp.	Nazwa zbioru danych <i>(np. dane klientów, pracowników itd.)</i>	Struktura zbiorów <i>(np. imię i nazwisko, e-mail, telefon itd.)</i>	Przeływ danych <i>(np. wydruk danych z Internetu)</i>	Uwagi
1.	Akta osobowe pracowników Centrum Usług Wspólnych w Okonku	Awans zawodowy, ocena pracy, imię, nazwisko, numer i seria dowodu osobowego, nip, adres zamieszkania/zameldowania/korespondencja, wykształcenie, orzeczenia lekarskie, świadectwa pracy, umowy, nagrody, zmiany płacowe, numer telefonu, nazwisko rodowe, nazwisko panięskie matki, imię ojca matki, stan cywilny, dane rodziców, badania BHP, awans zawodowy, dane płacowe, książeczki zdrowia,	brak	
2.	Akta osobowe dyrektorów placówek podlegających pod CUW	Awans zawodowy, ocena pracy, imię, nazwisko, numer i seria dowodu osobowego, nip, adres zamieszkania/zameldowania/korespondencja, wykształcenie, orzeczenia lekarskie, świadectwa pracy, umowy, nagrody, zmiany płacowe, numer telefonu, nazwisko rodowe, nazwisko panięskie matki, imię ojca matki, stan cywilny, dane rodziców, badania BHP, awans zawodowy, dane płacowe, książeczki zdrowia,	brak	
3.	Ewidencja czasu pracy	Imię, nazwisko, pesel, data urodzenia, NIP,	Z wersji papierowej na wersje papierową; z wersji papierowej na wersję elektroniczną	
4.	Listy płac pracowników CUW i jednostek podlegających CUW	Imię, nazwisko, pesel, numer rachunku bankowego	Z wersji papierowej na wersje papierową; z wersji	

Lp.	Nazwa zbioru danych <i>(np. dane klientów, pracowników itd.)</i>	Struktura zbiorów <i>(np. imię i nazwisko, e-mail, telefon itd.)</i>	Przebieg danych <i>(np. wydruk danych z Internetu)</i>	Uwagi
5	Dane pracownicze do ubezpieczenia	Imię, nazwisko, adres, data i miejsce urodzenia, pesel, imiona rodziców, nazwisko rodowe matki, nr i seria dowodu osobistego, imię nazwisko członka rodziny, nr telefonu, wykształcenie	papierowej na wersję elektroniczną Z wersji papierowej na wersje papierową; z wersji papierowej na wersję elektroniczną	
6	Dokumentacja wypadkowa pracowników CUW i jednostek podlegających pod CUW	Imię, nazwisko, adres, data i miejsce urodzenia, pesel, nr i seria dowodu osobistego, rodzaj uszczerbku na zdrowiu	Z wersji papierowej na wersje papierową	
7	Dokumentacja emerytalno rentowa, RP -7	Imię, nazwisko, adres, data i miejsce urodzenia, pesel, imiona rodziców, nazwisko rodowe matki, nr i seria dowodu osobistego, przebieg zatrudnienia, RP7	Z wersji papierowej na wersje papierową	
8	Dokumentacja związana z organizacją staży zawodowych, praktyk	Imię, nazwisko, adres, data i miejsce urodzenia, pesel, nr i seria dowodu osobistego	Z wersji papierowej na wersje papierową	
9	Umowy cywilno prawne, prace zlecenia na rzecz szkoły	Imię, nazwisko, adres, numer konta bankowego, imię, nazwisko dziecka, data urodzenia, pesel, dane firmy,	Z wersji papierowej na wersje papierową	
10	Zbiór danych do SIO	Imię, nazwisko, adres, data i miejsce urodzenia, pesel, imiona rodziców, adres zamieszkania/zameldowania nr telefonu	Z wersji papierowej na wersje papierową, z wersji papierowej na wersje elektroniczną	
11	Obowiązki szkolny	Imię, nazwisko, data i miejsce urodzenia, pesel, imiona rodziców, adres zamieszkania/zameldowania	Z wersji papierowej na wersje papierową	
12	Dotacje dla placówek niepublicznych	Imię, nazwisko, adres, numer rachunku bankowego, data urodzenia, pesel, dane firmy	Z wersji papierowej na wersje papierową	

Lp.	Nazwa zbioru danych <i>(np. dane klientów, pracowników itd.)</i>	Struktura zbiorów <i>(np. imię i nazwisko, e-mail, telefon itd.)</i>	Przebieg danych <i>(np. wydruk danych z Internetu)</i>	Uwagi
13	Dowody księgowo CUW oraz jednostek podlegających pod CUW	Imię, nazwisko, adres, pesel, numer rachunku bankowego, NIP, nazwa firmy, data urodzenia	Z wersji papierowej na wersje papierową, z wersji papierowej na wersje elektroniczną	
14	Organizacja dowozu	Imię, nazwisko, adres, pesel	Z wersji papierowej na wersje papierową	
15	Dokumentacja rozliczeniowa z ZUS -Płatnik	Imię, nazwisko, adres, data i miejsce urodzenia, pesel, imiona rodziców, nazwisko rodowe matki, imię i nazwisko członka rodziny	Z wersji papierowej na wersje papierową, z wersji elektronicznej na wersje elektroniczną	
16	Dziennik korespondencji	Imię, nazwisko, adres, dane firmy, treść wystanej korespondencji, data	brak	
17	Zalecenia pokontrolne	Wynik kontroli, nazwa organu kontrolującego, adres, imię i nazwisko, zalecenia pokontrolne	Z wersji papierowej na wersje papierową	
18	Wnioski o nagrody, medale, odznaczenia	Imię i nazwisko	Z wersji papierowej na wersje papierową	
19	Skierowania na badania	Imię i nazwisko, adres, pesel, stanowisko	Z wersji papierowej na wersje papierową	
20	Sprawozdania z wykonania budżetu, plany finansowe	Imię i nazwisko, stanowisko	Z wersji papierowej na wersje papierową, z wersji elektronicznej na wersje elektroniczną	
21	Dokumenty założycielskie jednostki	Imię i nazwisko, adres, NIP, pesel	Z wersji papierowej na wersje papierową	
22	Ewidencja placówek niepublicznych	Imię i nazwisko, nazwa firmy, NIP, Regon, pesel. Adres, nr telefonu, e-mail	Z wersji papierowej na wersje papierową	
23	Inwentaryzacja	Imię i nazwisko, stanowisko	Z wersji papierowej na wersje papierową	

Lp.	Nazwa zbioru danych <i>(np. dane Klientów, pracowników itd.)</i>	Struktura zbiorów <i>(np. imię i nazwisko, e-mail, telefon itd.)</i>	Przeptyw danych <i>(np. wydruk danych z Internetu)</i>	Uwagi
24	Bilans jednostek	Imię i nazwisko, stanowisko	Z wersji papierowej na wersje papierową	
25	Zaświadczenia o dochodach, zatrudnieniu CUW i jednostek	Imię i nazwisko, pesel, data i miejsce urodzenia, imię i nazwisko rodziców, adres	Z wersji papierowej na wersje papierową	
26	Potrącenia z wynagrodzenia CUW i jednostek	Imię i nazwisko	Z wersji papierowej na wersje papierową	
27	Pracownicy młodociani	Imię i nazwisko, adres, NIP, nr telefonu, nazwa firmy, data i miejsce urodzenia, PKD, wykształcenie, zawód	Z wersji papierowej na wersje papierową, z wersji elektronicznej na wersje elektroniczną	
28	Godziny ponadwymiarowe	Imię i nazwisko	Z wersji papierowej na wersje papierową	
29	Absencja w pracy, rejestr zwolnień lekarskich	Imię i nazwisko, pesel, data urodzenia	Z wersji papierowej na wersje papierową, z wersji elektronicznej na wersje elektroniczną	
30	ZFŚS CUW	Imię i nazwisko, pesel, data urodzenia, adres, stanowisko, imię i nazwisko członków rodziny oraz data urodzenia,	Z wersji papierowej na wersje papierową	

Data i podpis Administratora Bezpieczeństwa Informacji

.....**ANSPEN/TO-R**.....
ds. księgowości i budżetowej

Katarzyna Kot

**Upoważnienie do przetwarzania danych osobowych załącznik nr 5 do „Polityki Bezpieczeństwa”
zgodnie z Art 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.**

Dyrektor **RENATA ZABROCKA** jako Administrator Danych
dnia 02.01.2017 r. nadaje upoważnienie do przetwarzania danych osobowych
w podmiocie **CENTRUM USŁUG WSPÓLNYCH W OKONKU** dla:

Imię i nazwisko: **ALEKSANDRA MIKOŁAJEWSKA**
Adres zamieszkania: **UL. SZCZECIŃSKA 5/7 64-965 OKONEK**
Nr PESEL: **63080201886**
Stanowisko służbowe: **GŁÓWNA KSIĘGOWA**

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich
przetwarzania:

**Dane pracownicze, kadrowe, płacowe oraz księgowość, dane pracownicze udostępnione innym
podmiotom, dane pracownicze do ZUS, umowy cywilno prawne, faktury, dane nauczycieli, zbiór
danych do SIO, dokumentacja oświadczeń ubezpieczeniowych, dane pracownicze do funduszu
świadczeń socjalnych, arkusz organizacyjny, listy osób, bilans, sprawozdania, BESTIA, Home banking
– przelewy.**

Upoważnienie nadaje się na czas pełnienia obowiązków służbowych

Ja niżej podpisany zobowiązuje się do przestrzegania zasad panujących w podmiocie w zakresie ochrony danych
osobowych a w szczególności „Polityki Bezpieczeństwa” oraz respektowania zapisów **Ustawy o ochronie danych
osobowych z dnia 29 sierpnia 1997 r.** Upoważnionego zobowiązuje się do zapewnienia ochrony danych,
zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w podmiocie oraz sposobów zabezpieczeń
a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2016 r.
poz. 922 z późn. zm.) oraz Rozporządzenia 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 ze zm.).

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów Rozdziału 8 Ustawy o ochronie
danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych
przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w podmiocie
może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować
odpowiedzialnością dyscyplinarną.

DYREKTOR
Administrator Danych
Centrum Usług Wspólnych
w Okonku

Renata Zabrocka
Podpis

Użytkownik
GŁÓWNA KSIĘGOWA

Aleksandra Mikołajewska

**Upoważnienie do przetwarzania danych osobowych załącznik nr 5 do „Polityki Bezpieczeństwa”
zgodnie z Art 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.**

Dyrektor **RENATA ZABROCKA** jako Administrator Danych
dnia 02.01.2017 r. nadaje upoważnienie do przetwarzania danych osobowych
w podmiocie **CENTRUM USŁUG WSPÓLNYCH W OKONKU** dla:

Imię i nazwisko: **MARIA WIŚNIEWSKA**
Adres zamieszkania: **UL. NIEPODLEGŁOŚCI 64A/1 64-965 OKONEK**
Nr PESEL: **59062306122**
Stanowisko służbowe: **INSPEKTOR DS. KADR**

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich
przetwarzania:

**Akta osobowe, dane pracownicze, kadrowe, płacowe, dane pracownicze udostępnione innym
podmiotom, dane pracownicze do ZUS, umowy cywilno prawne , dokumentacja emerytalno -
rentowa.**

Upoważnienie nadaje się na czas pełnienia obowiązków służbowych

Ja niżej podpisany zobowiązuje się do przestrzegania zasad panujących w podmiocie w zakresie ochrony danych
osobowych a w szczególności „Polityki Bezpieczeństwa” oraz respektowania zapisów **Ustawy o ochronie danych
osobowych z dnia 29 sierpnia 1997 r.** Upoważnionego zobowiązuje się do zapewnienia ochrony danych,
zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w podmiocie oraz sposobów zabezpieczeń
a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2016 r.
poz. 922 z późn. zm.) oraz Rozporządzenia 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 ze zm.).

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów Rozdziału 8 Ustawy o ochronie
danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych
przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w podmiocie
może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować
odpowiedzialnością dyscyplinarną.

DYREKTOR
Centrum Usług Wspólnych
Administrator Danych

Renata Zabrocka

Podpis

Użytkownik

INSPEKTOR
ds. Kadr

Maria Wiśniewska

Centrum Usług Wspólnych
Okonku, ul. Leśna 41.
64-965 OKONEK
71 7 04 789 REGON:36605228
145 67 2669 715

**Upoważnienie do przetwarzania danych osobowych załącznik nr 5 do „Polityki Bezpieczeństwa”
zgodnie z Art 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.**

Dyrektor **RENATA ZABROCKA** jako Administrator Danych
dnia 02.01.2017 r. nadaje upoważnienie do przetwarzania danych osobowych
w podmiocie **CENTRUM USŁUG WSPÓLNYCH W OKONKU** dla:

Imię i nazwisko: **KATARZYNA KOT**
Adres zamieszkania: **UL. WODNA 21/3 64-965 OKONEK**
Nr PESEL: **84061405701**
Stanowisko służbowe: **INSPEKTOR DS. KADR**

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich
przetwarzania:

**Dane pracownicze, kadrowe, płacowe oraz księgowość, dane pracownicze udostępnione innym
podmiotom, dane pracownicze do ZUS, umowy cywilno prawne, faktury, dane nauczycieli,
dokumentacja oświadczeń ubezpieczeniowych, dane pracownicze do funduszu świadczeń
socjalnych, listy osób, Home banking – przelewy.**

Upoważnienie nadaje się na czas pełnienia obowiązków służbowych

Ja niżej podpisany zobowiązuje się do przestrzegania zasad panujących w podmiocie w zakresie ochrony danych
osobowych a w szczególności „Polityki Bezpieczeństwa” oraz respektowania zapisów **Ustawy o ochronie danych
osobowych z dnia 29 sierpnia 1997 r.** Upoważnionego zobowiązuje się do zapewnienia ochrony danych,
zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w podmiocie oraz sposobów zabezpieczeń
a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2016 r.
poz. 922 z późn. zm.) oraz Rozporządzenia 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 ze zm.).

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów Rozdziału 8 Ustawy o ochronie
danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych
przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w podmiocie
może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować
odpowiedzialnością dyscyplinarną.

DYREKTOR
Centrum Usług Wspólnych
Administrator Danych

Renata Zabrocka

.....
Podpis

Użytkownik
ds. księgowości budżetowej

Katarzyna Kot

**Upoważnienie do przetwarzania danych osobowych załącznik nr 5 do „Polityki Bezpieczeństwa”
zgodnie z Art 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.**

Dyrektor **RENATA ZABROCKA** jako Administrator Danych
dnia 02.01.2017 r. nadaje upoważnienie do przetwarzania danych osobowych
w podmiocie **CENTRUM USŁUG WSPÓLNYCH W OKONKU** dla:

Imię i nazwisko: **EWA LUBERDA**
Adres zamieszkania: **UL. SZCZECIŃSKA 5/16 64-965 OKONEK**
Nr PESEL: **56031812888**
Stanowisko służbowe: **INSPEKTOR DS. PŁAC**

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich przetwarzania:

Akta osobowe, dane pracownicze, kadrowe, płacowe oraz księgowość, dane pracownicze udostępnione innym podmiotom, dane pracownicze do ZUS, umowy cywilnoprawne, zbiór danych do SIO, dokumentacja ubezpieczeniowa, dane pracownicze.

Upoważnienie nadaje się na czas pełnienia obowiązków służbowych

Ja niżej podpisany zobowiązuje się do przestrzegania zasad panujących w podmiocie w zakresie ochrony danych osobowych a w szczególności „Polityki Bezpieczeństwa” oraz respektowania zapisów **Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.** Upoważnionego zobowiązuje się do zapewnienia ochrony danych, zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w podmiocie oraz sposobów zabezpieczeń a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 z późn. zm.) oraz Rozporządzenia 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 ze zm.).

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów Rozdziału 8 Ustawy o ochronie danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w podmiocie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Administrator Danych
Centrum Usług Wspólnych
w Okonku

Renata Zbrocka
Podpis

Użytkownik

INSPEKTOR

Ewa Luberda

**Upoważnienie do przetwarzania danych osobowych załącznik nr 5 do „Polityki Bezpieczeństwa”
zgodnie z Art 37 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.**

Dyrektor **RENATA ZABROCKA** jako Administrator Danych
dnia 02.01.2017 r. nadaje upoważnienie do przetwarzania danych osobowych
w podmiocie **CENTRUM USŁUG WSPÓLNYCH W OKONKU** dla:

Imię i nazwisko: **STANASIUK DANASIUK**
Adres zamieszkania: **UL. LEŚNA 26 64-965 OKONEK**
Nr PESEL: **60091805560**
Stanowisko służbowe: **INSPEKTOR DS. PŁAC ROZLICZEŃ MATERIAŁOWYCH**

Upoważniony otrzymuje dostęp do poniższych zasobów danych osobowych w celu ich
przetwarzania:

**Akta osobowe, dane pracownicze, kadrowe, płacowe oraz księgowość, dane pracownicze
udostępnione innym podmiotom, wnioski o nagrody, obowiązek szkolny, dane pracownicze do
ZUS, dokumentacja naboru, umowy cywilnoprawne, zbiór danych do SIO, sprawozdania,
dotacje, ewidencja placówek niepublicznych, organizacja dowozu.**

Upoważnienie nadaje się na czas pełnienia obowiązków służbowych

Ja niżej podpisany zobowiązuje się do przestrzegania zasad panujących w podmiocie w zakresie ochrony danych
osobowych a w szczególności „Polityki Bezpieczeństwa” oraz respektowania zapisów **Ustawy o ochronie danych
osobowych z dnia 29 sierpnia 1997 r.** Upoważnionego zobowiązuje się do zapewnienia ochrony danych,
zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w podmiocie oraz sposobów zabezpieczeń
a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2016 r.
poz. 922 z późn. zm.) oraz Rozporządzenia 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 ze zm.).

Oświadczam, że zostałem(am) poinformowany o grożącej, stosownie do przepisów Rozdziału 8 Ustawy o ochronie
danych osobowych, odpowiedzialności karnej. Niezależnie od odpowiedzialności przewidzianej w wymienionych
przepisach, mam świadomość, że naruszenie zasad ochrony danych osobowych, obowiązujących w podmiocie
może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować
odpowiedzialnością dyscyplinarną.

DYREKTOR
Administrator Danych
Centrum Usług Wspólnych
w Okonku

.....
Renata Zbrocka

Podpis

Użytkownik
Inspektor ds. płac

.....
Danuta Stanasiuk

Ewidencja osób przetwarzających dane w podmiocie posiadających upoważnienie

załącznik nr 6 do „Polityki Bezpieczeństwa” zgodnie z Art 39. 1. Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

Lp.	Imię i nazwisko	Stanowisko służbowe	Data nadania upoważnienia	Data ustania upoważnienia	Wykaz zbiorów danych wynikających z upoważnienia	Identyfikator (Jeżeli dane są przetwarzane w systemie informatycznym)
1	Zabrocka Renata	dyrektor	02.01.2017	Na czas pełnienia obowiązków służbowych	Akta osobowe, dane pracownicze, kadrowe, płacowe oraz księgowość, dane pracownicze udostępnione innym podmiotom, wnioski o nagrody, obowiązek szkolny, dane pracownicze do ZUS, dokumentacja naboru, umowy cywilno prawne, zbiór danych do SIO, sprawozdania, dotacje, ewidencja placówek niepublicznych, organizacja dowozu.	dyrektor
2	Stanasiuk Danuta	Inspektor ds. plac i rozliczeń materiałowych	02.01.2017	Na czas pełnienia obowiązków służbowych	Akta osobowe, dane pracownicze, kadrowe, płacowe oraz księgowość, dane pracownicze udostępnione innym podmiotom, dane pracownicze do ZUS, umowy cywilno prawne, zbiór danych do SIO, dokumentacja ubezpieczeniowa, dane pracownicze.	Danuta
3	Luberda Ewa	Inspektor ds. plac	02.01.2017	Na czas pełnienia obowiązków służbowych	Akta osobowe, dane pracownicze, kadrowe, płacowe oraz księgowość, dane pracownicze udostępnione innym podmiotom, dane	Ewa

Lp.	Imię i nazwisko	Stanowisko służbowe	Data nadania upoważnienia	Data ustania upoważnienia	Wykaz zbiorów danych wynikających z upoważnienia	Identyfikator <i>(Jeżeli dane są przetwarzane w systemie informatycznym)</i>
					pracownicze do ZUS, umowy cywilno prawne, Płatnik, dokumentacja ubezpieczeniowa, dane pracownicze.	
4	Mikołajewska Aleksandra	Główna Księgowa	02.01.2017	Na czas pełnienia obowiązków służbowych	Dane pracownicze, kadrowe, płacowe oraz księgowość, dane pracownicze udostępnione innym podmiotom, dane pracownicze do ZUS, umowy cywilno prawne, faktury, dane nauczycieli, zbiór danych do SIO, dokumentacja oświadczeń ubezpieczeniowych, dane pracownicze do funduszu świadczeń socjalnych, arkusz organizacyjny, listy osób, bilans, sprawozdania, BESTIA, Home banking – przelewy.	Ola
5	Kot Katarzyna	Inspektor ds. księgowości budżetowej	02.01.2017	Na czas pełnienia obowiązków służbowych	Dane pracownicze, kadrowe, płacowe oraz księgowość, dane pracownicze udostępnione innym podmiotom, dane pracownicze do ZUS, umowy cywilno prawne, faktury, dane nauczycieli, dokumentacja oświadczeń ubezpieczeniowych, dane pracownicze do funduszu świadczeń socjalnych, listy osób, Home banking – przelewy.	Kot

Lp.	Imię i nazwisko	Stanowisko służbowe	Data nadania upoważnienia	Data ustania upoważnienia	Wykaz zbiorów danych wynikających z upoważnienia	Identyfikator <i>(Jeżeli dane są przetwarzane w systemie informatycznym)</i>
6	Wiśniewska Maria	Inspektor ds. kadr	02.01.2017	Na czas pełnienia obowiązków służbowych	Akta osobowe, dane pracownicze, kadrowe, placowe, dane pracownicze udostępnione innym podmiotom, dane pracownicze do ZUS, umowy cywilno prawne, dokumentacja emerytalno - rentowa.	Maria

Data i podpis Administratora Danych

.....**INSPEKTOR**.....
ds. księgowości budżetowej

Katarzyna Kot

DYREKTOR
Centrum Usług Wspólnych
w Okoniu

Renata Zabrocka

załącznik nr 7 do „Polityki Bezpieczeństwa” zgodnie z art. 38 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

Zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Lp.	Rodzaj udostępnionych danych osobowych	Data wprowadzenia danych do zbioru	Data przekazania danych osobowych	Imię i nazwisko osoby która otrzymała dane	Cel przekazania danych osobowych
1.	faktury	codziennie	codziennie	księgowość	rozrachunkowy
2.	Dokumenty do ZUS	co miesiąc	co miesiąc	Dział placowy	Rozrachunkowo - ewidencyjny
3.	Dokumenty (umowy o pracę, umowy zlecenie, nadgodziny, premie, dodatek motywacyjny, wynagrodzenie dodatkowe)	co miesiąc	co miesiąc	Dział placowy i księgowość	rozrachunkowy
4.	SIO	zgodnie z harmonogramem	zgodnie z harmonogramem		ewidencyjny
5.	Wyprawka szkolna	zgodnie z harmonogramem	zgodnie z harmonogramem	Dział placowy i księgowość	rozrachunkowo-ewidencyjny
6.	Pracownicy młodociani	zgodnie z harmonogramem	zgodnie z harmonogramem	Burmistrz Okonka	ewidencyjny
7.	Dotacje	co miesiąc	co miesiąc	Burmistrz Okonka	rozrachunkowo-ewidencyjny
8.	Dane do SIO	zgodnie z harmonogramem	zgodnie z harmonogramem	Dyrektorzy placówek	rozrachunkowo-ewidencyjny
9.	Listy wynagrodzeń	co miesiąc	co miesiąc	Dyrektorzy placówek	ewidencyjny
10.	Informacja roczna dla osoby ubezpieczeniowej	raz w roku	raz w roku	Dyrektorzy placówek	ewidencyjny
11.	Informacja roczna o dochodach oraz pobranych zaliczkach na podatek dochodowy	raz w roku	raz w roku	Dyrektorzy placówek	ewidencyjny
12.	Sprawozdania z wykonania budżetu	co miesiąc	co miesiąc	Dyrektorzy placówek	rozrachunkowo-ewidencyjny
13.	Zaświadczenia o dochodach	na potrzebę pracowników	na potrzebę pracowników	Pracownicy poszczególnych placówek	ewidencyjny

14.	Ewidencja placówek niepublicznych	na wniosek	na wniosek	wnioskujący podmiot	ewidencyjny
15.	Upoważnienia do SIO	na wniosek	na wniosek	wnioskujący pracownik	ewidencyjny

Data i podpis Administratora Bezpieczeństwa Informacji

01.01.2017

INSPEKTOR
ds. księgowości budżetowej

Katarzyna Kót