**Zarządzenie Nr 4/2016**

**Kierownika Ośrodka Pomocy Społecznej w Kobylinie-Borzymach**

**z dnia 14 czerwca 2016 roku**

w sprawie ustalenia i wdrożenia Polityki bezpieczeństwa przetwarzania danych osobowych i danych wrażliwych w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach oraz instrukcji zarządzania systemem informatycznym.

 Na podstawie ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz. U. z 2015r., poz.2135 z późn. zm.) oraz Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004r. Nr 100, poz.1024) , Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbioru danych (Dz.U. z 2015 poz. 719) i Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji – zarządzam co następuje:

**§ 1.**

Wprowadza się „Politykę bezpieczeństwa przetwarzania danych osobowych i danych wrażliwych w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach’’ w brzmieniu stanowiącym załącznik Nr 1 do niniejszego zarządzenia.

**§ 2.**

Wprowadza się „Instrukcję zarządzania systemem informatycznym w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach’’ w brzmieniu stanowiącym załącznik Nr 2 do niniejszego zarządzenia.

**§ 3.**

Zobowiązuję się pracowników przetwarzających dane osobowe do przetwarzania reguł zawartych w dokumentach wymienionych w § 1 oraz § 2.

**§ 4.**

Traci moc Zarządzenie Nr 2/2013 Kierownika Ośrodka Pomocy Społecznej w Kobylinie-Borzymach z dnia 29 października 2013 r. w sprawie wprowadzenia Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach.

**§ 5.**

Zarządzenie wchodzi w życie z dniem podjęcia.

 Załącznik Nr 1/2016

 do Zarządzenia Nr 4/2016 Kierownika Ośrodka Pomocy Społecznej

 w Kobylinie Borzymach

 z dnia 14 czerwca 2016 r.

 **POLITYKA BEZPIECZEŃSTWA
I OCHRONY PRZETWARZANIA DANYCH OSOBOWYCH**

Dotyczy przetwarzania danych osobowych w formie tradycyjnej jak i za pośrednictwem systemów informatycznych.

**Dokumentację opracowano zgodnie z:**

* Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity: Dz. U. 2014 r.
poz. 1182 z późn. zm.*).
* Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.
(*Dz. U. z 2004 r. nr 100, poz. 1024*) w sprawie dokumentacji przetwarzania danych osobowych
oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
* Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. *(Dz. U. 2015 r. poz. 719)* w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.

 Zatwierdził

 . . . . . . . . . . . . . . . . . . . .

 Podpis Administratora

**ROZDZIAŁ I**

**Postanowienia ogólne**

§ 1

Użyte w Polityce Bezpieczeństwa określenia oznaczają:

1. **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,
2. **Administrator Danych Osobowych (ADO)** – Ośrodek Pomocy Społecznej reprezentowany przez Bożenę Piszczatowską,
3. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. **Stacja robocza** – stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie,
5. **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie,
6. **Osoba upoważniona** - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu (*wzór upoważnienia stanowi* ***załącznik nr 4*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych)* oraz wykazana w ewidencji upoważnień *(wzór ewidencji stanowi* ***załącznik nr 5*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych),*
7. **Użytkownik systemu** - osoba posiadająca uprawnienia do przetwarzania danych osobowych
w systemie informatycznym,
8. **Osoba uprawniona** - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych do wykonywania w jego imieniu określonych czynności,
9. **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*tekst jednolity: Dz. U.
2015 r. poz. 2135 z późn. zm.*).

§ 2

1. Najwyższe kierownictwo jest zaangażowane w zapewnienie bezpieczeństwa ochrony danych osobowych i w związku z tym:
	1. deklaruje, że zapewnienie realizacji działalności statutowej jednostki przy zachowaniu najwyższej staranności w zakresie bezpieczeństwa przetwarzania danych osobowych jest strategicznym celem jednostki,
	2. stosuje kompleksowe podejście do zagadnień związanych z bezpieczeństwem przetwarzania danych osobowych, gdyż tylko takie postępowanie gwarantuje skuteczność podejmowanych działań,
	3. podejmuje niezbędne działania w celu likwidacji słabych ogniw w systemie zabezpieczeń,
	4. śledzi osiągnięcia w dziedzinie bezpieczeństwa danych osobowych,
	5. wdraża nowe narzędzia i metody pracy mające na celu zwiększenie ochrony danych osobowych,
	6. zobowiązuje każdego pracownika jednostki do zapoznania się z Polityką Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych,
	7. deklaruje, że Polityka Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych będzie podlegała ciągłemu doskonaleniu w oparciu o analizy i oceny będące wynikiem sprawdzeń w zakresie przestrzegania w powyższym zakresie unormowań. Niezbędna aktualizacja będzie dokonywana również w wyniku zmian w przepisach prawnych, rozwoju technologii, a także zmian organizacyjnych warunkujących dokonanie takiej aktualizacji.
2. Realizując Politykę bezpieczeństwa i ochrony przetwarzania danych osobowych zapewnia się:
	1. poufność – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom,
	2. integralność – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany,
	3. dostępność – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie,
	przez autoryzowany podmiot,
	4. rozliczalność – możliwość jednoznacznego przypisania działań poszczególnym osobom,
	5. autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana,
	6. niezaprzeczalność – uczestnictwo w całości lub części wymiany danych przez jeden
	z podmiotów uczestniczących w tej wymianie jest niepodważalne,
	7. niezawodność – zamierzone zachowania i skutki są spójne,
3. Polityka bezpieczeństwa i ochrony przetwarzania danych osobowych ma na celu wyeliminowanie lub w przypadku braku możliwości, zmniejszenie prawdopodobieństwa zdarzenia oraz minimalizowania skali oddziaływania w przypadku ich wystąpienia w zakresie:
	1. naruszeń danych osobowych rozumianych jako prywatne dobro powierzone podmiotowi,
	2. naruszeń przepisów prawa oraz innych regulacji,
	3. utraty lub obniżenia reputacji podmiotu,
	4. strat finansowych ponoszonych w wyniku nałożonych kar,
	5. zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.

§ 3

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:
2. nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
3. wszelkie modyfikacje danych osobowych lub próby ich dokonania przez osoby nieuprawnione (*np. zmian zawartości danych, utrata bądź przejęcie całości lub części danych*),
4. naruszenie lub próby naruszenia integralności systemu,
5. zmianę lub utratę danych zapisanych na kopiach zapasowych,
6. naruszenie lub próby naruszenia poufności danych lub ich części,
7. nieuprawniony dostęp (*sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu*),
8. udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
9. zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji zmierzające do zakłócenia działania bądź pozyskania w sposób niedozwolony (*lub w celach niezgodnych z przeznaczeniem*) danych zawartych w systemach informatycznych lub kartotekach,
10. inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika
po zakończeniu pracy.
11. Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku
lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

§ 4

W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, użytkowników oraz oprogramowanie systemowe i aplikacje w przypadku przetwarzania danych za pomocą systemu informatycznego.

**ROZDZIAŁ II**

**Zarządzanie bezpieczeństwem danych osobowych**

§ 5

Za przetwarzanie danych osobowych niezgodne z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w Kodeksie pracy.

1. **Administrator Danych Osobowych (ADO)**:
	1. Jest odpowiedzialny za całość zagadnień dotyczących ochrony i bezpieczeństwa przetwarzania danych osobowych,
	2. Formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych
	przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
	3. Zarządzanie ryzykiem związanym z przetwarzaniem danych osobowych, poprzez stałe nadzorowanie jego poziomu, zmniejszanie prawdopodobieństwa jego zaistnienia oraz minimalizowania skali jego oddziaływania w przypadku gdy zaistniało.
	4. Prowadzi dokumentację opisującą ww. środki oraz sposób przetwarzania danych,
	5. Zapewnia kontrolę nad tym jakie dane, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
	6. Zapoznaje osoby upoważnione do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
	7. Wydaje upoważnienie do przetwarzania danych osobowych określając w nich zakres i termin ważności (*wzór upoważnienia określa* ***załącznik nr 4*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*),
	8. Prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych (*wzór ewidencji stanowi* ***załącznik nr 5*** *Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*), która zawiera:
		* 1. nazwę zbioru;
			2. imię i nazwisko osoby upoważnionej;
			3. identyfikator, jeżeli dane są przetwarzane w systemie informatycznym
			4. numer upoważnienia;
			5. datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
	9. Ewidencjonuje oświadczenia osób upoważnionych i zaznajomionych z zasadami zachowania bezpieczeństwa danych (*wzór ewidencji określa* ***załącznik nr 7*** *dokumentacji Polityki Bezpieczeństwa
	 i Ochrony Przetwarzania Danych Osobowych*).
	10. Decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych,
	11. Odpowiada za zgodne z prawem przetwarzanie danych osobowych,
2. **Pracownik Przetwarzający Dane**:
3. Zapoznaje się z zasadami określonymi w Polityce bezpieczeństwa i ochrony przetwarzania danych osobowych i Instrukcji zarządzania systemem informatycznym oraz składa oświadczenie o znajomości zawartych w nich przepisów.
4. Chroni prawo do prywatności osób powierzających swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce bezpieczeństwa i ochrony przetwarzania danych osobowych,
5. Przestrzega przepisów o ochronie danych osobowych, a także ściśle współpracuje z Administratorem Danych Osobowych oraz Administratorem Bezpieczeństwa Informacji.
6. Ma ukończone szkolenie w zakresie ochrony danych osobowych (lista uczestników szkolenia z zakresu ochrony danych osobowych znajduje się w załączniku nr 8 dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych),

**ROZDZIAŁ III**

**Identyfikacja zagrożeń bezpieczeństwa przetwarzania danych osobowych**

§ 6

Na podstawie przeprowadzonej identyfikacji zagrożeń przy przetwarzaniu danych osobowych wykazano następujące zagrożenia:

* + 1. włamania od strony okien – wybite szyby, niedomknięte skrzydła,
		2. włamania od strony drzwi – uszkodzone klamki, źle działające zamki, niedomknięte drzwi, ślady po narzędziach,
		3. oddziaływanie czynników zewnętrznych – pożar, zalanie pomieszczeń, katastrofa budowlana,
		4. pozostawienie niezamkniętych drzwi – jeżeli w pomieszczeniu nie pozostają osoby uprawnione do przetwarzania danych,
		5. pozostawienie bez nadzoru osób nieuprawnionych do przebywania w pomieszczeniach,
		6. pozostawienie danych na biurkach, półkach, regałach, itp. po zakończeniu pracy,
		7. pozostawienie dokumentów zawierających dane osobowe w kserokopiarce lub skanerze,
		8. pozostawienie po zakończeniu pracy otwartych szaf, w których gromadzone są dane osobowe,
		9. przechowywanie dokumentów w miejscach do tego nieprzeznaczonych,
		10. wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie,
		11. przetwarzanie danych przez osoby nieuprawione,
		12. nieuzasadnione sporządzanie kserokopii danych,
		13. dopuszczenie zapisywania na nośniki zewnętrzne wynoszone poza obszar przetwarzania lub przesyłanie poprzez Internet danych niezaszyfrowanych,
		14. dopuszczanie do nieuzasadnionego kopiowania dokumentów i utraty kontroli nad kopią,
		15. sporządzanie kopii danych w sytuacjach niewynikających z zakresu obowiązków służbowych,
		16. utrata kontroli nad kopią danych osobowych,
		17. podmiana lub zniszczenie nośników z danymi osobowymi,
		18. pozostawienie zapisanego hasła dostępu do bazy danych,
		19. samodzielne instalowanie oprogramowania, którego instalacja nie jest wymagana w celu umożliwienia wykonywania obowiązków służbowych,
		20. obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania,
		21. opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do danych osobowych,
		22. odczytywanie nośników przed sprawdzeniem ich programem antywirusowym,
		23. dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania osób nieuprawnionych,
		24. ujawnianie sposobu działania aplikacji oraz jej zabezpieczeń osobom niepowołanym,
		25. ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej,
		26. dopuszczenie aby inne osoby odczytywały zawartość ekranu monitora,
		na którym wyświetlane są dane osobowe,
		27. awarie sprzętu i oprogramowania, które mogą wskazywać na działanie osób trzecich,
		28. nieoczekiwane, niedające się wyjaśnić zmiany zawartości bazy danych,
		29. niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych,
		30. próba nieuzasadnionego przeglądania danych w ramach pomocy technicznej,
		31. dopuszczanie aby osoby inne niż ADO lub osoby przez niego uprawnione podłączały jakiekolwiek urządzenia, demontowały elementy sieci lub dokonywały innych manipulacji,
		32. manipulacja przy układach sieci komputerowej lub komputerach,
		33. obecność nowych urządzeń i kabli o nieznanym przeznaczeniu i pochodzeniu,

**ROZDZIAŁ IV**

**Ocena ryzyka**

§ 7

W celu zminimalizowania ryzyka, czyli możliwości wykorzystania podatności przez zagrożenie w celu spowodowania utraty zachowania poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności danych osobowych, a przez to negatywnego bezpośredniego lub pośredniego wpłynięcia na jednostkę dokonano oceny poziomu ryzyka.

Poziom ryzyka to iloczyn prawdopodobieństwa wystąpienia zdarzeń określonych w § 6 oraz skali oddziaływania (skutków) w przypadku ich wystąpienia.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Prawdopodo-bieństwo | 5Bardzo wysokie | 5 | 10 | 15 | 20 | 25 |
| 4Wysokie | 4 | 8 | 12 | 16 | 20 |
| 3Średnie | 3 | 6 | 9 | 12 | 15 |
| 2Niskie | 2 | 4 | 6 | 8 | 10 |
| 1Bardzo niskie | 1 | 2 | 3 | 4 | 5 |
|  |  | 1Bardzo małe | 2Małe | 3Średnie | 4Duże | 5Bardzo duże |
|  |  | Oddziaływanie |

Poziom ryzyka określa zależność:

**R=P\*O**

gdzie:

R – poziom ryzyka,

P – prawdopodobieństwo wystąpienia zdarzenia,

O – skala oddziaływania w przypadku wystąpienia zdarzenia,

Z punktu widzenia jednostki najbardziej istotne są obszary, w których poziom ryzyka wynosi więcej niż 15. Jest to ryzyko nieakceptowalne, które musi zostać zmniejszone i stale monitorowane. W przypadku wystąpienia takiego poziomy przetwarzanie danych zostaje wstrzymane do momentu jego zmniejszenia.

Poziom ryzyka w skali od 4 do 14 oznaczono obszar średniego zagrożenia.

Poziom ryzyka od 1 do 3 to obszar ryzyka, w którym zmaterializowanie się zdarzeń jest mało prawdopodobne, lub ich wpływ na jednostkę jest niewielki.

§ 8

|  |  |  |  |
| --- | --- | --- | --- |
| Zagrożenie: | Prawdopodobieństwo: | Oddziaływanie: | Poziom ryzyka: |
| włamania od strony okien | 1 | 3 | 3 |
| włamania od strony drzwi | 1 | 3 | 3 |
| oddziaływanie czynników zewnętrznych | 1 | 3 | 3 |
| pozostawienie niezamkniętych drzwi | 1 | 3 | 3 |
| pozostawienie bez nadzoru osób nieuprawnionych do przebywania w pomieszczeniach | 1 | 2 | 2 |
| pozostawienie danych na biurkach, półkach, regałach, itp. po zakończeniu pracy | 1 | 2 | 2 |
| pozostawienie dokumentów zawierających dane osobowe w kserokopiarce lub skanerze | 1 | 2 | 2 |
| pozostawienie po zakończeniu pracy otwartych szaf, w których gromadzone są dane osobowe | 1 | 2 | 2 |
| przechowywanie dokumentów w miejscach do tego nieprzeznaczonych | 1 | 1 | 1 |
| wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie | 1 | 2 | 2 |
| przetwarzanie danych przez osoby nieuprawione | 1 | 2 | 2 |
| nieuzasadnione sporządzanie kserokopii danych | 1 | 2 | 2 |
| dopuszczenie zapisywania na nośniki zewnętrzne wynoszone poza obszar przetwarzania lub przesyłanie poprzez Internet danych niezaszyfrowanych | 1 | 2 | 2 |
| dopuszczanie do nieuzasadnionego kopiowania dokumentów i utraty kontroli nad kopią | 1 | 1 | 1 |
| sporządzanie kopii danych w sytuacjach niewynikających z zakresu obowiązków służbowych | 1 | 2 | 2 |
| utrata kontroli nad kopią danych osobowych | 1 | 2 | 2 |
| podmiana lub zniszczenie nośników z danymi osobowymi | 1 | 2 | 2 |
| pozostawienie zapisanego hasła dostępu do bazy danych | 1 | 3 | 3 |
| samodzielne instalowanie oprogramowania, którego instalacja nie jest wymagana w celu umożliwienia wykonywania obowiązków służbowych | 1 | 2 | 2 |
| obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania | 1 | 2 | 2 |
| opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do danych osobowych | 1 | 2 | 2 |
| odczytywanie nośników przed sprawdzeniem ich programem antywirusowym | 1 | 2 | 2 |
| dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania osób nieuprawnionych | 1 | 3 | 3 |
| ujawnianie sposobu działania aplikacji oraz jej zabezpieczeń osobom niepowołanym | 1 | 2 | 2 |
| dopuszczenie aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe | 2 | 1 | 2 |
| awarie sprzętu i oprogramowania, które mogą wskazywać na działanie osób trzecich | 1 | 2 | 2 |
| nieoczekiwane, niedające się wyjaśnić zmiany danych | 1 | 2 | 2 |
| niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych | 1 | 2 | 2 |
| próba nieuzasadnionego przeglądania danych w ramach pomocy technicznej | 1 | 2 | 2 |
| dopuszczanie aby osoby inne niż ADO, lub osoby przez niego uprawnione podłączały jakiekolwiek urządzenia, demontowały elementy sieci lub dokonywały innych manipulacji | 1 | 3 | 3 |
| manipulacja przy układach sieci komputerowej lub komputerach | 1 | 3 | 3 |
| obecność nowych urządzeń i kabli o nieznanym przeznaczeniu i pochodzeniu | 1 | 3 | 3 |

Jak przedstawia powyższa analiza, poziom ryzyka w jednostce jest niski (maksymalny poziom ryzyka wynikający z macierzy wynosi 3). Oznacza to więc, iż zastosowane środki techniczne oraz organizacyjne mające na celu zapewnienie bezpieczeństwa i ochronę danych osobowych są wystarczające.

Pomimo takiej oceny, nie należy zaprzestać analizowania jego poziomu. Trzeba aktualizować jego ocenę każdorazowo w przypadku jakiejkolwiek zmiany w sposobie przetwarzania danych osobowych lub zmianach spowodowanych wprowadzeniem nowych środków organizacyjnych określonych w niniejszej dokumentacji lub technicznych (określonych w załączniku nr 3 dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych).

Obowiązkiem Administratora Danych Osobowych jest również stałe podnoszenie wiedzy oraz umiejętności w celu wyeliminowania ryzyka szczątkowego, poprzez stałe prace nad zmniejszeniem prawdopodobieństwa zdarzenia oraz minimalizowania skali oddziaływania w przypadku ich wystąpienia

**ROZDZIAŁ V**

**Przetwarzanie danych osobowych**

§ 9

1. Przetwarzanie danych osobowych ma miejsce wyłącznie gdy:
	1. jest to niezbędne do realizacji uprawnień, lub spełnienia obowiązków wynikających z przepisów prawa,
	2. jest to niezbędne do zrealizowania umowy, gdy osoba, której dane dotyczą, jest jej stroną lub jest to konieczne do podjęcia działań przed zawarciem umowy,
	3. jest konieczne do wykonania określonych prawnie zadań realizowanych dla dobra publicznego,
	4. jest to konieczne di wypełniania prawnie usprawiedliwionych celów realizowanych przez jednostkę, a przetwarzanie nie narusza praw i wolności osób, której dane dotyczą,
	5. osoba, której dane dotyczą, wyrazi pisemną zgodę na przetwarzanie danych osobowych. Zgoda nie może być domniemana lub dorozumiana. Zgoda musi być dobrowolna i zawarta z zachowaniem równowagi pomiędzy dającym zgodę, a Administratorem Danych Osobowych,
2. W przypadku legalności przetwarzania danych wynikających z pkt. 1, pkt a - d jednostka nie musi występować o zgodę na przetwarzanie danych osobowych,
3. Zabrania się przetwarzania danych wrażliwych, chyba że jest to dopuszczalne w oparciu o przepis szczególny ustawy innej niż Ustawa o Ochronie Danych Osobowych i zachowana jest pełna gwarancja ochrony tych danych,

§ 10

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą Administrator Danych Osobowych informuje tę osobę o:
	1. pełnej nazwie i adresie siedziby Administratora Danych Osobowych,
	2. celu zbierania danych, w szczególności o znanych mu, w czasie udzielania informacji, odbiorcach lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
	3. prawie dostępu do treści swoich danych oraz ich poprawiania,
	4. dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej,
2. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą Administrator Danych Osobowych informuje tę osobę:
	1. pełnej nazwie i adresie siedziby Administratora Danych Osobowych,
	2. celu zbierania danych, w szczególności o znanych mu, w czasie udzielania informacji, odbiorcach lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
	3. źródle danych,
	4. prawie dostępu do treści swoich danych oraz ich poprawiania,
	5. przysługującym prawie do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych Administratora, zgodnie z art. 32.1 Ustawy.
3. Obowiązek informacyjny wypełniany jest w chwili zbierania danych.
4. Administrator Danych Osobowych posiada pisemne potwierdzenia spełnienia obowiązku informacyjnego.
5. Obowiązku informacyjnego nie wypełnia się jeśli:
	1. przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania,
	2. osoba, której dane dotyczą, posiada przedmiotowe informacje.

§ 11

1. Na wniosek osoby, której dane dotyczą, Administrator Danych jest poinformować tę osobę na piśmie o prawach jej przysługujących oraz udzielić odnośnie do jej danych osobowych informacji:
	1. o tym jakie dane osobowe zawiera zbiór,
	2. kto jest administratorem danych,
	3. jaki jest cel, zakres i sposób przetwarzania danych zawartych w zbiorze,
	4. terminie od kiedy przetwarza się w zbiorze dane jej dotyczące,
	5. źródle, z którego pochodzą dane jej dotyczące, chyba, że Administrator Danych Osobowych jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej,
	6. o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane są udostępniane,
	7. przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2 Ustawy.
2. Administrator Danych odmawia osobie, której dane dotyczą udzielenia ww. informacji, jeżeli spowodowałoby to:
	1. ujawnienie wiadomości zawierających informacje niejawne,
	2. zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,
	3. zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,
	4. istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.
3. Wzór informacji o zawartości zbioru danych osobowych określa załącznik nr 13 dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych,

**Rozdział VI**

**Udostępnianie oraz powierzanie przetwarzania danych osobowych**

§ 12

Udostępnianie danych osobowych:

* 1. dane osobowe mogą być udostępniane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa,
	2. wzór wniosku o udostępnienie danych ze zbioru danych osobowych określa załącznik nr 15 dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych,
	3. Administrator Danych Osobowych zachowuje szczególną staranność i nadzór w zakresie udostępniania danych osobowych,
	4. udostępnienie danych nie może naruszać praw i wolności osób, których one dotyczą,
	5. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych jeżeli może to naruszyć bezpieczeństwo i ochronę danych,
	6. w celu nadzoru nad udostępnianiem danych osobowych prowadzona jest ewidencja udostępniania danych osobowych, której wzór określony jest w załączniku nr 16 dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych,

§ 13

Powierzanie przetwarzania danych osobowych:

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi w drodze pisemnej umowy,
2. do umów zawieranych z podmiotami zewnętrznymi zostają włączone klauzule dotyczące:
	1. dotyczące obowiązku ochrony tych informacji przez strony umowy zarówno w trakcie trwania umowy jak i po jej ustaniu,
	2. ograniczenia dostępu do informacji wyłącznie do osób związanych z realizacją umowy,
	3. zakazu ujawniania danych,
	4. odpowiedzialności w przypadku naruszenia bezpieczeństwa danych zarówno przez podmiot jak i zatrudnionych pracowników.
3. Umowy powierzenia przetwarzania danych zawierają:
	1. określenie celu i zakresu powierzenia przetwarzania danych osobowych,
	2. zasady przetwarzania i ochrony danych zgodnie z Ustawą,
	3. spełnienie wymogów wynikających z Ustawy,
	4. prawo kontroli spełnienia wymogów podmiotu, któremu powierzono dane,
	5. odpowiedzialność podmiotu i jego pracowników z tytułu powierzenia przetwarzania danych osobowych,
	6. obowiązek poinformowania o wszelkich naruszeniach w zakresie przetwarzania danych osobowych oraz kontrolach uprawnionych instytucji zewnętrznych,
	7. skutki naruszenia zasad przetwarzania danych osobowych,
	8. obowiązki podjęcia działań mających na celu zapobiegnięcie naruszenia ochrony danych osobowych oraz wdrożenie środków zapobiegawczych mających na celu brak możliwości wystąpienia naruszeń w przyszłości,
	9. informację o zwrocie danych osobowych w momencie zakończenia obowiązywania umowy,
	10. prawo do natychmiastowego rozwiązania umowy w przypadku braku przestrzegania jej postanowień
4. Podmiot, któremu powierzono przetwarzanie danych osobowych może przetwarzać te dane wyłącznie w zakresie i celu przewidzianym w umowie, ponosi również odpowiedzialność za zachowanie wszelkich wymogów wynikających z przepisów prawa w zakresie ochrony danych osobowych, w szczególności zastosowanie wymogów technicznych i organizacyjnych do zabezpieczenia przedmiotowych danych.

§ 14

1. Tradycyjne przetwarzanie danych osobowych oraz w systemach informatycznych w jednostce odbywa się wyłącznie na obszarze wyznaczonym przez Administratora Danych Osobowych (*wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe określa* ***załącznik nr 1*** *Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*).
2. Przetwarzanie danych osobowych za pomocą urządzeń przenośnych może odbywać się
poza obszarem przetwarzania danych wyłącznie za zgodą Administratora Bezpieczeństwa Informacji.

§ 15

W celu ograniczenia dostępu osób postronnych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych zapewniono:

1. wydawanie kluczy do pomieszczeń podlegające rejestracji, z jednoczesnym poświadczeniem przez osobę odbierającą faktu otrzymania kluczy o oznaczonym numerze (*wzór protokołu określa* ***załącznik nr 17*** *Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*),

2. pracownicy Administratora Danych Osobowych są zobowiązani do przestrzegania zasad określających dopuszczalne sposoby przemieszczania się osób trzecich w obrębie pomieszczeń, w których przetwarzane są dane osobowe, tzn:

* 1. stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe mają tylko osoby upoważnione,
	2. dostęp do pomieszczeń, w których przetwarzane są dane osobowe osób innych niż wymienione w pkt. 1 jest możliwy wyłącznie za pisemną zgodą Administratora Danych Osobowych,
	3. przebywanie osób upoważnionych po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą Administratora Danych Osobowych,
	4. wszyscy pracownicy zobowiązani są do zwracania uwagi na zachowanie osób wchodzących i wychodzących z jednostki,
	5. przebywanie osób trzecich w pomieszczeniach może odbywać się wyłącznie w obecności osób upoważnionych lub za pisemną zgodą Administratora Danych Osobowych.

§ 16

Szczegółowy wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych
do ich przetwarzania określa ***załącznik nr 1*** Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych.

§ 17

Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych
oraz sposób przepływu danych określa ***załącznik nr 2*** Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych.

**Rozdział VII**

**Sprawdzanie zgodności przetwarzania danych osobowych**

§ 18

1. Administrator Danych Osobowych zapewnia przestrzeganie zasad ochrony danych osobowych.
2. Administrator Danych Osobowych dokonuje okresowych sprawdzeń i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.
3. Sprawdzenie przeprowadzane jest w trybie:
	* 1. sprawdzenia planowego - według planu sprawdzeń określającego przedmiot, zakres oraz termin przeprowadzania poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania (*wzór planu sprawdzeń określa* ***załącznik nr 9*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*),
		2. sprawdzenia doraźnego - w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez Administratora Danych Osobowych wiadomości o naruszeniu ochrony danych osobowych (*wzór zgłoszenia podejrzenia naruszenia ochrony danych osobowych określa* ***załącznik nr 13*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*) lub uzasadnionego podejrzenia wystąpienia takiego naruszenia,
4. Ze sprawdzeń, o których mowa w ust. 3, sporządza się sprawozdanie (*wzór sprawozdania określa* ***załącznik nr 10*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*).
5. Sprawdzenia, o których mowa w ust. 3 są ewidencjonowane (rejestr sprawdzeń i oceny funkcjonowania mechanizmów zabezpieczeń oraz zasad postępowania w przypadku naruszenia ochrony danych osobowych określa załącznik nr 11 dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych).
6. Administrator Danych Osobowych w planie sprawdzeń uwzględnia, w szczególności, zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych:
	1. z zasadami, o których mowa w art. 23- 37 i art. 31- 35 Ustawy,
	2. z zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 36, art. 37- 39 Ustawy, w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
	3. z zasadami przekazywania danych osobowych, o których mowa w art. 47- 48 ustawy,
	4. z obowiązkiem zgłoszenia zbioru danych do rejestracji i jego aktualizacji, jeżeli zbiór zawiera dane, o których mowa w art. 27 ust. 1 ustawy.
7. Plan sprawdzeń przygotowywany jest na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan ten zawiera co najmniej jedno sprawdzenie.
8. Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem raz na pięć lat.
9. Sprawdzenie doraźne przeprowadza się niezwłocznie po powzięciu wiadomości przez ADO o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.
10. Administrator Danych Osobowych dokumentuje czynności zgodnie z § 4 Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.

**Rozdział VIII**

**Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych**

§ 19

1. Przed przystąpieniem do pracy osoba upoważniona zobowiązana jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
2. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik systemu zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora Danych Osobowych.
3. Obowiązek określony w ust. 2 ciąży również na pozostałych pracownikach Administratora Danych Osobowych.
4. Postanowienia ust. 2 i 3 mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemach informatycznych,
jak i w formie tradycyjnej.

§ 20

1. Do czasu przybycia Administratora Danych Osobowych zgłaszający:
2. powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności mogących spowodować zatarcie lub naruszenie śladów
bądź innych dowodów,
3. zabezpiecza elementy systemu informatycznego lub dokumentacji, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym,
4. podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
5. Postanowienia ust. 1 mają zastosowanie zarówno w przypadku naruszenia, jak i w przypadku podejrzenia naruszenia ochrony danych.

§ 21

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych Administrator Danych Osobowych po przybyciu na miejsce:

1. ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane oraz stan urządzeń, a także identyfikuje wielkość negatywnych następstw incydentu,
2. wysłuchuje relacji osoby, która dokonała powiadomienia,
3. podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

§ 22

1. Administrator Danych Osobowych sporządza z przebiegu zdarzenia sprawozdanie (*wzór sprawozdania określa* ***załącznik nr 10*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*), w którym powinny się znaleźć w szczególności informacje o:
2. dacie i godzinie powiadomienia,
3. godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane,
4. sytuacji, jaką zastał,
5. podjętych działaniach i ich uzasadnieniu.

§ 23

1. Administrator Danych Osobowych podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczeń danych osobowych i zapobieżenia wystąpieniu ich w przyszłości. W tym celu:
	1. w miarę możliwości przywraca stan zgodny z zasadami zabezpieczenia systemu,
	2. o ile taka potrzeba zachodzi, postuluje wprowadzenie nowych form zabezpieczenia, a w razie ich wprowadzenia nadzoruje zaznajamianie z nimi osób zatrudnionych przy przetwarzaniu danych osobowych.
2. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej dyscypliny pracy, Administrator Danych Osobowych podejmuje stosowne działania wobec osób, które dopuściły się tego uchybienia.

§ 24

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia
od Administratora Danych Osobowych.

§ 25

1. W przypadku zaginięcia komputera lub nośników, na których były zgromadzone dane osobowe, użytkownik systemu niezwłocznie powiadamia Administratora Danych Osobowych, a w przypadku kradzieży występuje o powiadomienie jednostki policji.
2. W sytuacji, o której mowa w ust. 1 Administrator Danych Osobowych, podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajęcia, który powinna podpisać także osoba, której skradziono lub której zaginął sprzęt.
3. W przypadku kradzieży komputera razem z nośnikiem magnetycznym lub elektronicznym Administrator Danych Osobowych podejmuje działania zmierzające do odzyskania utraconych danych oraz monitoruje proces przebiegu wyjaśnienia sprawy.

§ 26

Osoba zatrudniona przy przetwarzaniu danych osobowych odpowiedzialna za naruszenie obowiązków wynikających z niniejszej Polityki bezpieczeństwa oraz przepisów o ochronie danych osobowych ponosi odpowiedzialność przewidzianą w Regulaminie pracy, Kodeksie pracy oraz wynikających z ustawy
o ochronie danych osobowych.

**ROZDZIAŁ IX**

**Postępowanie w wypadku klęski żywiołowej**

§ 27

Klęską żywiołową jest katastrofa spowodowana działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.

§ 28

W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób
lub mienia z pomieszczeń, w których przetwarzane są dane osobowe mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.

§ 29

* + - 1. Każda osoba, która będzie świadkiem zbliżania się lub działania zagrożeń określonych w §26 zobowiązana jest powiadomić Danych Osobowych w każdy możliwy sposób.
			2. Numer telefonu Administratora Danych Osobowych jest znany pracownikom.

§ 30

Osoby biorące udział w akcji ratunkowej, mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe bez dopełniania obowiązku, o którym mowa w §10.

 § 31

W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy przebywający w pomieszczeniach,
w których przetwarzane są dane osobowe obowiązani są do przerwania pracy, a w miarę możliwości przed opuszczeniem tych pomieszczeń do:

* 1. zamknięcia systemu informatycznego,
	2. zabezpieczenia danych osobowych przetwarzanych tradycyjnie.

§ 32

1. W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator Danych Osobowych oraz obecni użytkownicy powinni w miarę możliwości zabezpieczać dane osobowe przed nieuprawnionym do nich dostępem, o ile nie stoi to w sprzeczności z poleceniami wydanymi przez służby ratunkowe.
2. Obowiązek ten ciąży w równym stopniu na innych pracownikach Administratora Danych Osobowych obecnych przy akcji ratunkowej.

**ROZDZIAŁ X**

**Niszczenie danych osobowych**

§ 33

Usuwanie danych osobowych, polega na:

1. trwałym, fizycznym ich zniszczeniu wraz z ich nośnikami w stopniu uniemożliwiającym
ich odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod,
2. anonimizacji zbiorów danych osobowych polegającej na pozbawieniu danych osobowych,
ich zbiorów – cech umożliwiających identyfikację osób fizycznych, których dane dotyczą.

Procedura niszczenia danych osobowych:

1. niszczenie danych osobowych następuje wyłącznie na wniosek Administratora Danych Osobowych,
2. sposób zniszczenia danych osobowych musi być odpowiednio dobrany do rodzaju nośnika danych oraz ich kategorii,
3. niszczenie danych osobowych musi odbywać się komisyjnie, przy czym w komisji musi znajdować się Administrator Danych Osobowych,
4. zniszczenie danych osobowych musi zostać potwierdzone spisaniem protokołu (*wzór protokołu określa* ***załącznik nr 16*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*).

Usuwanie danych osobowych jest zależne od rodzaju nośnika, na którym są przechowywane.

1. Dokumentacja tradycyjna (wydruki, notatki, dokumenty itd.) niezawierająca danych wrażliwych – przy użyciu niszczarki kategorii P-3 lub wyższej (zgodnie z normą **DIN 66399**),
2. Dokumentacja tradycyjna (wydruki, notatki, dokumenty itd.) zawierająca dane wrażliwe – przy użyciu niszczarki kategorii P-4 (zgodnie z normą **DIN 66399**),
3. Nośniki optyczne (płyty CD/DVD/BLU-RAY – analogicznie do dokumentacji tradycyjnej, za pomocą niszczarek, przy czym do danych niewrażliwych kategorii O-3 lub wyższej, a do danych wrażliwych kategorii O-4 (zgodnie z normą **DIN 66399**),
4. Nośniki elektroniczne (pendrive/karty pamięci/dyski twarde SSD) – korzystając z jednej z dwóch metod:
	* 1. niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych,
		2. niszczenie sprzętowe – polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń,
5. Nośniki magnetyczne (dyskietki/dyski twarde HDD) – korzystając z jednej z trzech metod:
	* 1. niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych,
		2. niszczenie sprzętowe – polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń, oprócz sposobów niszczenia danych dostępnych dla nośników elektronicznych,
		3. demagnetyzacji nośników,

**ROZDZIAŁ XI**

**Postanowienia końcowe**

§ 34

Polityka Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.

§ 35

1. Każda osoba przetwarzająca dane osobowe zobowiązana jest do zapoznania się z treścią Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych oraz do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień w nich zawartych.
2. Osoba upoważniona zobowiązana jest złożyć oświadczenie o tym, że została zaznajomiona
z przepisami ustawy o ochronie danych osobowych, wydanymi na jej podstawie aktami wykonawczymi, obowiązującą Polityką Bezpieczeństwa służącymi do przetwarzania danych osobowych (*wzór oświadczenia stanowi* ***załącznik nr 6*** *dokumentacji Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych*).
3. Oświadczenia przechowywane są w aktach osobowych pracownika.
4. Wszyscy pracownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych procedur i zasad zawartych w niniejszej dokumentacji.

**Załącznik nr 1**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

WYKAZ ZBIORÓW DANYCH PRZETWARZANYCH TRADYCYJNIE I W SYSTEMIE INFORMATYCZNYM
ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH
I MIEJSCEM PRZETWARZANIA

|  |  |  |  |
| --- | --- | --- | --- |
| l.p. | Nazwa zbioru danych | Lokalizacja zbioru danych osobowych(budynek, pomieszczenie) | Nazwa programu zastosowanego do przetwarzania danych oraz autor programu |
|  | Pomoc społeczna | Ośrodek Pomocy Społecznej Kobylin – Borzymy, ul. Główna 11 budynek Urzędu Gminy pokój nr 11-12 | Helios - INFOR |
|  | Świadczenia rodzinne | Ośrodek Pomocy Społecznej Kobylin – Borzymy, ul. Główna 11 budynek Urzędu Gminy pokój nr 11-12 | Amazis - INFOR |
|  | Fundusz alimentacyjny | Ośrodek Pomocy Społecznej Kobylin – Borzymy, ul. Główna 11 budynek Urzędu Gminy pokój nr 11-12 | Nemezis - INFOR |
|  | Rejestr korespondencji | Ośrodek Pomocy Społecznej Kobylin – Borzymy, ul. Główna 11 budynek Urzędu Gminy pokój nr 11-12 | W formie rejestru - papierowo |
|  | Rejestr wyjść | Ośrodek Pomocy Społecznej Kobylin – Borzymy, ul. Główna 11 budynek Urzędu Gminy pokój nr 11-12 | W formie rejestru - papierowo |
|  | Stypendia szkolne i zasiłki szkolne | Ośrodek Pomocy Społecznej Kobylin – Borzymy, ul. Główna 11 budynek Urzędu Gminy pokój nr 11-12 | Tales - INFOR |
|  | Przeciwdziałanie przemocy w rodzinie | Ośrodek Pomocy Społecznej Kobylin – Borzymy, ul. Główna 11 budynek Urzędu Gminy pokój nr 11-12 | W formie papierowej |
|  | Karta Dużej Rodziny  | Ośrodek Pomocy Społecznej Kobylin – Borzymy, ul. Główna 11 budynek Urzędu Gminy pokój nr 11-12 | Karta Dużej Rodziny na platformie P.W.P.W.  |
|  | Wspieranie rodziny i piecza zastępcza | Ośrodek Pomocy Społecznej Kobylin – Borzymy, ul. Główna 11 budynek Urzędu Gminy pokój nr 11-12 | W formie papierowej  |
|  | **Rejestr pracowników zatrudnionych w OPS** | Ośrodek Pomocy Społecznej Kobylin – Borzymy, ul. Główna 11 budynek Urzędu Gminy pokój nr 11-12 | Program kadry i płace 2013.3.20.6.14Płatnik 8.01.001A |
|  | Przeciwdziałanie uzależnieniom | Ośrodek Pomocy Społecznej Kobylin – Borzymy, ul. Główna 11 budynek Urzędu Gminy pokój nr 11-12 | W formie papierowej |
|  | Zbiór danych kontrahentów w OPS zawiera informacje o kontrahentach w OPS wartości i przedmiocie umowy | Ośrodek Pomocy Społecznej Kobylin – Borzymy, ul. Główna 11 budynek Urzędu Gminy pokój nr 11-12 | Program przelewy |
|  | Rodzina 500+ | Ośrodek Pomocy Społecznej Kobylin – Borzymy, ul. Główna 11 budynek Urzędu Gminy pokój nr 11-12 | Izyda - INFOR |

**Załącznik nr 2**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Kobylinie-Borzymach

Opis struktury zbioru danych osobowych przetwarzanych TRADYCYJNIE I w systemach informatycznych ORAZ sposób przepływu danych pomiędzy systemami informatycznymi

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Nazwa zbioru danych | Opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze | Opis przepływu danych |
|  | Pomoc społeczna | Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, NIP, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, nr telefonu, nr konta bankowego, stan cywilny, płeć, obywatelstwo, stan rodziny, informacje o opłatach i alimentach ,informacje o dochodzie na zasadach ogólnych, dochodzie utraconym, zryczałtowanym, nieopodatkowanym. | Z Ośrodka Pomocy Społecznej do Banku BS Zambrów/ o Kobylin-Borzymy na nośniku zewnętrznym. |
|  | Świadczenia rodzinne | Imię i nazwisko, data urodzenia, adres miejsca zamieszkania lub pobytu, numer PESEL, numer dokumentu potwierdzający tożsamość, stan cywilny, obywatelstwo, stopień pokrewieństwa z członkami rodziny, rodzaj szkoły, do której uczęszcza dziecko, orzeczenie o niepełnosprawności lub stopniu niepełnosprawności, liczbę wysokość wypłaconych świadczeń, płeć, dochody, organ do którego złożono wniosek rodzaj wnioskowanego świadczenia oraz datę złożenia wniosku,  | Z Ośrodka Pomocy Społecznej do Banku BS Zambrów/ o Kobylin-Borzymy na nośniku zewnętrznym. |
|  | Fundusz alimentacyjny | Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, NIP, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, nr telefonu, nr konta bankowego, stan cywilny, płeć, obywatelstwo, stan rodziny, informacje o opłatach i alimentach ,informacje o dochodzie na zasadach ogólnych, dochodzie utraconym, zryczałtowanym, nieopodatkowanym. | Z Ośrodka Pomocy Społecznej do Banku BS Zambrów/ O Kobylin-Borzymy na nośniku zewnętrznym. |
|  | Rejestr korespondencji | Tytuł przesyłki, nadawca, adresat, data widniejąca na przesyłce, data wpływu i wysłania przesyłki do jednostki, znak sprawy widniejący na przesyłce, sposób otrzymania przesyłki, podpis osoby przekazującej przesyłkę | Nie ma przepływu danych pomiędzy poszczególnymi systemami informatycznymi służącymi do przetwarzania danych osobowych. |
|  | Stypendia szkolne i zasiłki szkolne | nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce pracy, seria i numer dowodu osobistego, stan cywilny, obywatelstwo, stopień niepełnosprawności, wysokość dochodów, stan rodzinny, stan zdrowia, inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym, miejsce nauki, imiona i nazwiska rodziców (opiekunów prawnych), rodzaj świadczenia o jakie ubiega się wnioskodawca, dane uzasadniające przyznanie pomocy, wysokość dochodów, informacja o korzystaniu z pomocy OPS, informacja o alimentach, ciężka choroba, niepełnosprawność, leczenie szpitalne, potwierdzenie zdarzenia losowego, nr rachunku bankowego, ilość ha prowadzonego gospodarstwa rolnego lub aktualny nakaz płatniczy, uzależnienia dowody opłacenia składek ZUS, podatku, informacja o wychowywaniu w rodzinie niepełnej  | Z Ośrodka Pomocy Społecznej do Banku BS Zambrów/ o Kobylin-Borzymy na nośniku zewnętrznym. |
|  | Przeciwdziałanie przemocy w rodzinie | nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, NIP, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, przekonania religijne, przekonania filozoficzne, przynależność wyznaniową, stan zdrowia, nałogi, życie seksualne, skazania, mandaty karne, orzeczenia o ukaraniu, inne orzeczenia wydane w postępowaniach sądowych lub administracyjnych. | Nie ma przepływu danych pomiędzy poszczególnymi systemami informatycznymi służącymi do przetwarzania danych osobowych |
|  | Karta Dużej Rodziny | Imię i nazwisko, PESEL, data urodzenia, adres zamieszkania (wnioskodawcy, data urodzenia, adres zamieszkania, stopień niepełnosprawności (członkowie rodziny) numer dokumentu, nazwa szkoły, nr telefonu | Przepływ danych odbywa się automatycznie za pomocą strony internetowej |
|  | Wspieranie rodziny i piecza zastępcza | Imię i nazwisko, data urodzenia, obywatelstwo, adres zamieszkania, stan cywilny, wykształcenie, zawód, miejsce pracy, źródło dochodu, dane dotyczące warunków mieszkaniowych, dane dotyczące sytuacji prawnej oraz aktualne miejsce pobytu dziecka, dane o rozwoju psychofizycznym dziecka. | Nie ma przepływu danych pomiędzy poszczególnymi systemami informatycznymi służącymi do przetwarzania danych osobowych |
|  | **Rejestr pracowników zatrudnionych w OPS** | Imię i nazwisko, adres zamieszkania, PESEL, NIP, numer dowodu osobistego, wykształcenie, stan cywilny, data i miejsce urodzenia, numer konta bankowego | Ręczne przeniesienie plików z systemu księgowego do systemu bankowego. |
|  | Przeciwdziałanie uzależnieniom | Imię i nazwisko, stan cywilny, data i miejsce urodzenia, miejsce zamieszkania, miejsce pracy, źródło utrzymania, nałogi, numer telefonu, sytuacja zawodowa, ekonomiczna, rodzinna, mieszkaniowa, zdrowotna, sytuacja dzieci. | Nie ma przepływu danych pomiędzy poszczególnymi systemami informatycznymi służącymi do przetwarzania danych osobowych |
|  | Zbiór danych kontrahentów w OPS zawiera informacje o kontrahentach w OPS wartości i przedmiocie umowy | Nazwa firmy, adres, NIP, numer faktury, numer telefonu, numer konta bankowego, data i termin płatności, wartość | Nie ma przepływu danych pomiędzy poszczególnymi systemami informatycznymi służącymi do przetwarzania danych osobowych |
|  | Rodzina 500+ | Imię i nazwisko, datę urodzenia, adres miejsca zamieszkania, miejsce zamieszkania, numer PESEL, stan cywilny, obywatelstwo, numer i serię dokumentu potwierdzającego tożsamość, stopień pokrewieństwa z członkami rodziny, orzeczenie o niepełnosprawności lub o stopniu niepełnosprawności, liczbę i wysokość opłaconych świadczeń, płeć, dochody, organ do którego złożono wniosek, oraz datę złożenia wniosku, organ który przyznał świadczenie, datę wydania decyzji oraz numer tej decyzji, okres na jaki świadczenie przyznano. | Z Ośrodka Pomocy Społecznej do Banku BS Zambrów/ o Kobylin-Borzymy na nośniku zewnętrznym. |

**Załącznik nr 3**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

WYKAZ ŚRODKÓW TECHNICZNYCH ZASTOSOWANYCH W CELU ZAPEWNIENIA BEZPIECZEŃSTWA
I OCHRONY DANYCH OSOBOWYCH:

|  |  |  |  |
| --- | --- | --- | --- |
| Nazwa pomieszczenia | Zabezpieczenia pomieszczenia | Zabezpieczenia zbiorów | Zabezpieczenia komputerów |
| Budynek Urzędu Gminy ul. Główna 11, 18-204 Kobylin-Borzymy nr pokoju: 11-12 | Alarm, okna PCV, drzwi drewniane zamykane na klucz | Teczki przechowywane w szafach drewnianych zamykanych na klucz | Programy antywirusowe, system wymuszający zmianę hasła, generator prądu, ustawienie monitora w sposób uniemożliwiający wgląd osób nieupoważnionych |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Załącznik 4**do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

 Kobylin-Borzymy , dnia 14 czerwca 2016r

. . . . . . . . . . . . . . . . . . . . . . . . . .

 (pieczątka

**Upoważnienie**

do przetwarzania danych osobowych nr: **1/2016**

Na podstawie art. 37 ustawy z dn 29 sierpnia 1997 roku o ochronie danych osobowych

(t.j. Dz. U. 2015, poz. 2135 z pózn. zm.) upoważniam

  **Panią …………………**

|  |  |  |
| --- | --- | --- |
| Adres: | PESEL: | Stanowisko: |
|  |  | **Starszy pracownik socjalny** |

do przetwarzania danych osobowych w następującym zakresie:

( nazwy zbiorów oraz zakres upoważnienia) [zbieranie/utrwalanie/przechowywanie/opracowywanie/zmienianie/udostępnianie/usuwanie/wgląd]

|  |  |
| --- | --- |
| Nazwa zbioru: | Zakres upoważnienia |
| Pomoc społeczna | Zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, wgląd |
| Rejestr korespondencji | Zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, wgląd |
| Rejestr wyjść | Zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, wgląd |
| Stypendia szkolne i zasiłki szkolne | Zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, wgląd |
| Przeciwdziałanie przemocy w Rodzinie | Zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, wgląd |
| Karta Dużej Rodziny | Zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, wgląd |
| Wspieranie Rodziny i piecza zastępcza | Zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, wgląd |

 Upoważnienie udzielane jest na czas pełnienia obowiązków pracowniczych od dnia 14.06.2016 r.

 Upoważniony zobowiązuje się do przestrzegania zasad panujących w jednostce w zakresie ochrony danych osobowych a w szczególności „Polityki Bezpieczeństwa„ oraz respektowania zapisów Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity: Dz. U. 2015 r. poz. 2135 z późn. zm.)

 Upoważnionego obowiązuje tajemnica dotycząca danych osobowych przetwarzanych w jednostce oraz sposobów zabezpieczeń.

 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

 (data i podpis Administratora Danych Osobowych) (data i podpis pracownika )

**Załącznik nr 5**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach.

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| L.p. | Zbiór danych osobowych | Nazwisko i imię / identyfikator | Numer upoważnienia | Data nadania (*modyfikacji*) upoważnienia | Data utraty ważności upoważnienia | Zakres upoważnienia do przetwarzania danych osobowych |
| 1 | Pomoc społeczna | Sikorska Urszula |  |  |  | Zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, wgląd. |
| 2. |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Załącznik nr 6** do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

. . . . . . . . . . . . . . . . . . . . . . . . .

 (dane pracownika)

OŚWIADCZENIE

Oświadczam, że zapoznałem(łam) się z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą z 29 sierpnia 1997r. o ochronie danych osobowych
(*tekst jednolity: Dz. U. 2015 r. poz. 2135 z późn. zm.*) oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące
do ich przestrzegania (*Dz. U. 2004 r. Nr 100, poz. 1024*).

Oświadczam ponadto, że zapoznałem(łam) się z Polityką Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach wprowadzoną dnia 14 czerwca 2016 roku przez Kierownika Ośrodka Pomocy Społecznej

Równocześnie oświadczam, iż znany jest mi telefoniczny numer kontaktowy do Administratora Danych Osobowych.

 Zobowiązuję się do:

* stosowania określonych przez ADO zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne w stosunku do celu przetwarzanie danych,
* należyte zabezpieczanie danych osobowych przed ich udostępnianiem osobom nieupoważnionym,
* zachowania szczególnej staranności w trakcie dokonywania operacji przetwarzania danych w celu ochrony osób, których dane dotyczą,
* zachowania tajemnicy danych oraz ich sposobu zabezpieczeń, nawet po ustaniu stosunku pracy.

 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

 (data i podpis)

**Załącznik nr 7**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

**EWIDENCJA OSÓB**

zapoznanych z „Polityką Bezpieczeństwa Przetwarzania i Ochrony Danych Osobowych”
w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach zapisami zawartymi w ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997r. (*tekst jednolity: Dz. U. 2015 r. poz. 2135 z późn. zm.*) oraz Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

**PRZYJĄŁEM/AM DO WIADOMOŚCI I STOSOWANIA ZAPISY**

**POLITYKI BEZPIECZEŃSTWA I INSTRUKCJI ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI**

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwisko i imię | Data i podpis |
| 1 | Sikorska Urszula |  |
| 2 | Kurzyna Małgorzata |  |
| 3 | Choińska Magda |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Załącznik nr 8**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

LISTA UCZESTNIKÓW SZKOLENIA Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

Prowadzący: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Miejsce i data szkolenia: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

|  |  |  |  |
| --- | --- | --- | --- |
| **L.p.** | **Imię uczestnika:** | **Nazwisko uczestnika:** | **Podpis:** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Załącznik nr 9**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

PLAN SPRAWDZEŃ W OŚRODKU POMOCY SPOŁECZNEJ W KOBYLINIE-BORZYMACH

NA OKRES od

Plan określa przedmiot, zakres oraz termin przeprowadzenia poszczególnych sprawdzeń w rozumieniu art. 36c ustawy o ochronie danych osobowych oraz ich zakres.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lp. | Przedmiot sprawdzenia: | Zakres sprawdzenia: | Termin sprawdzenia: | Sposób dokumentowania: | Zakres dokumentowania: |
| 1 | Realizacja procedur wdrożonych przez ADO w zakresie ochrony danych osobowych | * Ustawienie sprzętu komputerowego w pomieszczeniach – czy uniemożliwia dostęp do ekranu monitorów osobom postronnym
* Polityka czystego biurka
* Polityka kluczy
* Sprawdzenie czy osoby dopuszczone do przetwarzania danych osobowych otrzymały pisemne upoważnienia oraz oświadczenia o zapoznaniu z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osób dopuszczonych do przetwarzania danych osobowych
* Ustalamy, czy osoby, które nie powinny mieć już prawa dostępu do danych osobowych (np. byli pracownicy) mają odwołane upoważnienia
* Ewidencja wydanych upoważnień oraz jej zgodność z wydanymi upoważnieniami
 |  |  |  |
| 2 | Funkcjonowanie zastosowanych zabezpieczeń fizycznych oraz funkcjonowanie systemów zabezpieczeń systemowych | * Spełnienie wymogów z poziomu ochrony systemów informatycznych służących do przetwarzania danych osobowych przed osobami trzecimi
* Sprawdzenie mechanizmów automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika
* Sprawdzenie czy zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie
* Przestrzeganie zasady rozpoczęcia i zakończenia pracy w systemie
* Zabezpieczenie systemowe i fizyczne sprzętu komputerowego
* Tworzenie kopii zapasowych
* Odnotowywanie przez systemy służące do przetwarzania danych osobowych czynności wykonywane na danych osobowych przez użytkowników
 |  | Notatka, protokół |  |
| 3. | Prawidłowość funkcjonowania mechanizmów kontroli dostępu do zbioru danych | * Dostęp pracowników do zbiorów danych oraz zakres dostępu pracowników i weryfikacja wydanych upoważnień (w tym byłych pracowników oraz odwołanie upoważnień)
* Zasady nadawania (zmieniania) odbierania uprawnień do systemów informatycznych
* Stosowanie identyfikatorów i haseł dla użytkowników zgodnie z wymogami formalnymi
 |  |  |  |
| 4. | Inwentaryzacja dokumentacji opisującej sposób przetwarzania danych osobowych | * Zgodność dokumentacji przetwarzania danych z obowiązującymi przepisami prawa (rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004r. (Dz.U. z 2004 r., poz.1024) art. 39a ustawy
 |  |  |  |
| 5. | Weryfikacja zbioru/ów danych osobowych (należy wskazać zbiór/zbiory podlegające sprawdzeniu | * Sprawdzamy, czy wszystkie dane są przetwarzane legalnie, czyli czy został spełniony jeden z warunków postawionych w art. 23 ust.1 ustawy
* Sprawdzamy, czy instytucja wypełnia należycie obowiązek informacyjny wynikający z art. 24 ustawy
 |  |  |  |

**Dokumentowanie czynności w toku sprawdzenia zawiera w szczególności:**

1. Sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
2. Odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem;
3. Sporządzeniu kopii otrzymanego dokumentu, sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
4. Sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

(Data i podpis Administratora Danych Osobowych)

**Załącznik nr 10**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

 Kobylin-Borzymy, dn. . . . . . . . . . .r.

**SPRAWOZDANIE**

ze sprawdzenia i oceny funkcjonowania mechanizmów zabezpieczeń oraz zasad postępowania
w przypadku naruszenia ochrony danych osobowych.

W dniu . . . . . . . . . . . . . . . . , sprawdzający Bożena Piszczatowska- Kierownik Ośrodka Pomocy Społecznej w Kobylinie-Borzymach

w obecności osób asystujących: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

dokonał sprawdzenia w . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

W czasie kontroli stwierdzono i zalecono: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

/tu należy omówić wyniki sprawdzenia, np.: stanu zabezpieczenia systemów informatycznych oraz innych zbiorów danych jak i przestrzegania obowiązujących przepisów/procedur itp./.

Niniejsze sprawozdanie sporządzono w dwóch jednobrzmiących egzemplarzach i po odczytaniu podpisano.

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

 (podpisy osób asystujących) (podpis i pieczątka osoby przeprowadzającej sprawdzenie)

**Załącznik nr 11**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

REJESTR SPRAWDZEŃ I OCENY FUNKCJONOWANIA MECHANIZMÓW ZABEZPIECZEŃ
ORAZ ZASAD POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH
W OŚRODKU POMOCY SPOŁECZNEJ W KOBYLINIE-BORZYMACH

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| L.p. | Nazwa sprawdzanego działu | Nazwisko, imię i stanowisko osoby przeprowadzającej sprawdzenie | Czas trwania sprawdzenia | Uwagi | Podpis osoby przeprowadzającej sprawdzenie |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Załącznik nr 12**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

 Kobylin-Borzymy , dn. . . . . . . . . . .r.

. . . . . . . . . . . . . . . . . . . . . . . .

 (pieczątka )

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

*(imię i nazwisko)*

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

*(adres)*

**INFORMACJA**

**o zawartości zbioru danych osobowych**

W związku z Pani/Pana wnioskiem z dnia . . . . . . . . . . . . . r. o udzielenie informacji związanych
z przetwarzaniem danych osobowych w . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Działając na podstawie art. 33 ust. 1 Ustawy o ochronie danych osobowych informuję, że zbiór danych zawiera następujące Pani/Pana dane osobowe: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Powyższe dane przetwarzane są w . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

w celu . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

z zachowaniem wymaganych zabezpieczeń i zostały uzyskane . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Powyższe dane nie były/były udostępniane . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . *. . . . . . . . .* . .

w celu . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . *. . . . . . . . . .* .

 Zgodnie z rozdziałem 4 Ustawy o ochronie danych osobowych przysługuje Pani/Panu prawo
do kontroli danych osobowych, prawo ich poprawiania, a także w przypadkach kreślonych w art. 32 ust. 1 pkt 7 i 8 Ustawy, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz prawo sprzeciwu wobec przetwarzania danych w celach marketingowych lub wobec przekazywania danych innemu administratorowi danych osobowych.

 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

 (podpis Administratora Danych Osobowych)

**Załącznik nr 13**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

ZGŁOSZENIE

naruszenia bezpieczeństwa danych osobowych

w ……………………………………………

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

  *(dd.mm.rr)*  *(00:00)*

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

 ( imię i nazwisko, stanowisko służbowe )

3. Lokalizacja zdarzenia :

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

4. Opis zaistniałej sytuacji wpływającej na bezpieczeństwo danych osobowych:

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

 godz. i data przyjęcia zgłoszenia Podpis osoby zgłaszającej

 podpis Administratora

 Danych Osobowych

**Załącznik nr 14**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

**WNIOSEK**

**O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH**

1. Wniosek do: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

2. Wnioskodawca . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

 *(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy ew. NIP oraz REGON)*

3. Podstawa prawna upoważniająca do pozyskania danych:

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

4. Wskazanie przeznaczenia dla udostępnionych danych osobowych:

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

5. Oznaczenia lub nazwa zbioru, z którego mają być udostępnione dane osobowe:

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

6. Zakres żądanych informacji ze zbioru:

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych:

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

 (data i podpis wnioskodawcy)

**Załącznik nr 15**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

EWIDENCJA UDOSTĘPNIENIA DANYCH OSOBOWYCH

W OŚRODKU POMOCY SPOŁECZNEJ W KOBYLINIE-BORZYMACH

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| L.p. | Data wydania | Dane odbiorcy | Zakres udostępnionych danych | Podpis osobyudostępniającej dane osobowe |
| 1 | stale | Zakład Ubezpieczeń Społecznych |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Załącznik nr 16**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

. . . . . . . . . . . . . . . . . . . . . . . .

 Pieczątka

**Protokół zniszczenia danych osobowych**

**nr: . . . . . . . . . . . .**

1. Data operacji: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
2. Nazwa zbioru danych osobowych, z którego pochodzą dane: . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

1. Powód zniszczenia danych osobowych: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
2. Rodzaj nośnika z kopią zapasową: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
3. Sposób zniszczenia: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Skład komisji:

|  |  |  |
| --- | --- | --- |
| Imię i nazwisko: | Imię i nazwisko: | Imię i nazwisko: |
| ..............................................(podpis) | ..............................................(podpis) | ..............................................(podpis) |

**Załącznik nr 17**

do Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych

w Ośrodku Pomocy Społecznej w Kobylinie-Borzymach

Kobylin-Borzymy , dn. . . . . . . . . . .r.

**PROTOKÓŁ
PRZEKAZANIA/ZDANIA KLUCZY**

Data, godzina i miejsce odbioru: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

# Obecni :

 a) ze strony powierzającego: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

 *(imię i nazwisko)*

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

*(stanowisko)*

 b) ze strony odbierającego: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

 *(imię i nazwisko)*

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

*(stanowisko)*

# Przedmiot odbioru :

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

*(np. jeden komplet kluczy - 4 sztuki z czego 2 sztuki do kraty zabezpieczającej znajdującej się przed magazynem z zewnątrz i 2 sztuki do drzwi wejściowych do magazynu)*

Niniejszym zobowiązuję się do nieudostępniania ich osobom trzecim.

Przejęcie kluczy zobowiązuje mnie do odpowiedzialności materialnej podczas pobytu poza godzinami pracy.

Na tym protokół zakończono i po przeczytaniu podpisano

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

 Strona powierzająca Strona odbierająca