ZARZĄDZENIE WEWNĘTRZNE NR 14 / 2017 Z DNIA 30-06-2017r.

Administratora Danych Osobowych: Gmina Tczów w osobie: Andrzej Wolszczak w sprawie wprowadzenia Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym,

w związku z zapisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922) 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. z 2004 r. Nr 100, poz. 1024)

zarządza się, co następuje:

§1

Wprowadza się w podmiocie: **Gmina Tczów** „Politykę Bezpieczeństwa" oraz „Instrukcję Zarządzania Systemem Informatycznym".

§2

Zarządzenie jest adresowane do pracowników podmiotu: **Gmina Tczów** , wykonujących czynności określone w „Polityce Bezpieczeństwa" oraz „Instrukcji Zarzadzania Systemem Informatycznym". Każdy pracownik, zgodnie z wykazem, jest obowiązany zapoznać się z treścią „Polityki Bezpieczeństwa" i „Instrukcji Zarządzania Systemem Informatycznym".

§3

Administrator Danych Osobowych: Gmina Tczów w osobie: Andrzej Wolszczak zobowiązuje wszystkich pracowników do przestrzegania zapisów „Polityki Bezpieczeństwa" oraz stosowania się do „Instrukcji Zarządzania Systemem Informatycznym" pod groźbą konsekwencji służbowych, przewidzianych prawem.

§4

Niniejsze zarządzenie wchodzi w życie z dniem podpisania i ogłoszenia tj. z dniem **30-06-2017r**. Z kolei zarządzenie z dnia 30 września 1999r. w sprawie ochrony danych osobowych w Urzędzie Gminy w Tczowie traci moc obowiązywania z dniem **30-06-2017r.**

WÓJT

inż. Andrzej Wolszczak

.....

(podpis Administratora Danych Osobowych)

POLITYKA BEZPIECZEŃSTWA

Administrator Danych Osobowych – **Gmina Tczów**
w osobie: **Andrzej Wolszczak** dnia **30-06-2017r**

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 wchodzą w życie

z dniem **30-06-2017r** .

§ 1

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w podmiocie: **Gmina Tczów** , 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) **ADMINISTRATORZE BEZPIECZEŃSTWA INFORMACJI** – rozumie się przez to osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji. W przypadku nie powołania obowiązki wykonuje Administrator Danych Osobowych.
2) **ADMINISTRATORZE DANYCH OSOBOWYCH** – rozumie się przez to Administratora Danych Osobowych podmiotu reprezentowanego przez osobę kierującą,
3) **ADMINISTRATORZE SYSTEMU INFORMATYCZNEGO** – rozumie się przez to osobę, której Administrator Danych Osobowych powierzył pełnienie obowiązków administratora systemu,
4) **HAŚLE** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
5) **IDENTYFIKATORZE** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
6) **INTEGRALNOŚCI DANYCH** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
7) **ODBIORCY DANYCH** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela, o którym mowa w art. 31a ustawy, podmiotu, o którym mowa w art. 31 ustawy, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
8) **OSOBIE UPOWAŻNIONEJ DO PRZETWARZANIA DANYCH OSOBOWYCH** – rozumie się przez to osobę,

która upoważniona została do przetwarzania danych osobowych przez Administratora Danych Osobowych na piśmie zgodnie z art. 37 ustawy,

9) **POUFNOŚCI DANYCH** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

10) **PRZETWARZAJĄCYM** – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy,

11) **RAPORCIE** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,

12) **ROZLICZALNOŚCI** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

13) **ROZPORZĄDZENIU** – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. nr 100, poz. 1024),

14) **SIECI PUBLICZNEJ** – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. nr 100, poz. 1024),

15) **SIECI TELEKOMUNIKACYJNEJ** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. 2016 poz. 1489 z późn. zm.),

16) **SERWISANCIE** – rozumie się przez to firmę lub pracownika firmy zajmującej się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego i oprogramowania,

17) **SYSTEMIE INFORMATYCZNYM ADMINISTRATORA DANYCH** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,

18) **TELETRANSMISJI** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

19) **USTAWIE** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2016 r. poz. 922),

20) **UWIERZYTELNIANIU** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

21) **UŻYTKOWNIKU** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

§ 3

Administrator Danych Osobowych o nazwie: **Gmina Tczów** nie wyznacza **Administratora Bezpieczeństwa Informacji** celem 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 NR 1** do „Polityki Bezpieczeństwa".

§ 4

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe określa **ZAŁĄCZNIK NR 2** do „Polityki Bezpieczeństwa".

§ 5

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi wraz z przepływem danych pomiędzy poszczególnymi systemami określa **ZAŁĄCZNIK NR 3** do „Polityki Bezpieczeństwa".

§ 6

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

§ 7

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez **Administratora Danych Osobowych. Administrator Danych Osobowych** 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. Osobom, które nie przetwarzają danych osobowych, ale mają dostęp do obszaru przetwarzania danych osobowych, **Administrator Danych Osobowych** wydaje **zgody na przebywanie w obszarze przetwarzania – ZAŁĄCZNIK NR 4** do „Polityki Bezpieczeństwa". **Administrator Danych Osobowych** nadaje uprawnienia pracownikom, którzy przetwarzają dane poprzez podpisanie oświadczenia, które stanowi **ZAŁĄCZNIK NR 5** do „Polityki Bezpieczeństwa". Prowadzona jest dokumentacja opisująca sposób przetwarzania danych w podmiocie, a w szczególności:

1. ewidencja osób posiadających upoważnienie do przetwarzania danych osobowych, oraz przebywania w obszarze przetwarzania w podmiocie – **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".

§ 8

Administrator Danych Osobowych 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. Wzór umowy powierzenia danych osobowych określa **ZAŁĄCZNIK NR 9** do „Polityki Bezpieczeństwa".
Jeżeli **Administrator Danych Osobowych** nie powierza danych osobowych innemu podmiotowi, ale istnieją przesłanki na okoliczność zobowiązania drugiej strony do konieczności zachowania powziętych informacji w tajemnicy, stosuje się klauzulę poufności. Wzór klauzuli poufności określa **ZAŁĄCZNIK NR 10**.

§ 9

Na wniosek osoby, której dane dotyczą, **Administrator Danych Osobowych** jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach oraz udzielić, odnośnie do jej danych osobowych, informacji. Poza tym, Administrator Danych Osobowych w związku z art. 24 ust. 1, art. 25 ust. 1 i art. 32 ust. 1 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 2016 roku poz. 922) jest zobowiązany spełniać **obowiązek informacyjny**, którego treść określa **ZAŁĄCZNIK NR 11** do „Polityki Bezpieczeństwa".

§ 10

Administrator Danych Osobowych 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 Osobowych 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.

5. Celem Polityki bezpieczeństwa jest przetwarzanie zgodnie z przepisami danych osobowych przetwarzanych w podmiocie oraz ich ochrona przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed uszkodzeniem, zniszczeniem lub nieupoważnioną zmianą.

6. Ze względu na nieustannie zmieniające się zagrożenia przetwarzania danych o osobowych i zmiany prawa niniejsza polityka może być dokumentem dynamicznie zmieniającym się w czasie. Uaktualnienia procedur ochrony, oprogramowania i innych parametrów stosowanych przy przetwarzaniu danych osobowych znajdują na bieżąco odzwierciedlenie funkcjonalne w niniejszej Polityce.

7. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:
   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 Osobowych** 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 Osobowych** 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 Osobowych lub osoba przez niego upoważniona wdraża wszystkie niezbędne dokumenty wynikające z zapisów ustawy, oraz innych przepisów mających zastosowania przy przetwarzaniu danych osobowych.

Administrator Danych Osobowych

.....

Podpis

Tczów, dnia 30-06-2017r

UPOWAŻNIENIE DLA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI ORAZ ZAKRES OBOWIĄZKÓW

załącznik nr 1 do „Polityki Bezpieczeństwa"

Na podstawie § 3 Polityki Bezpieczeństwa z dnia **23-06-2017r,** zgodnie z założeniami
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

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 Osobowych (ADO): ***Gmina Tczów***

o numerze NIP: ***811-17-14-505***

powołuje / potwierdza powołanie **([1])**:

w osobie ***Andrzej Wolszczak***

Administratora Bezpieczeństwa Informacji (ABI): ***[IMIĘ I NAZWISKO]***

o numerze Pesel: ***[NR PESEL]***

Upoważnienie jest ważne od chwili podpisania przez strony do dnia wycofania upoważnienia 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 u.o.d.o., zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7 u.o.d.o. 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 u.o.d.o., 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

([1]) niepotrzebne usunąć

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 oraz posiadających upoważnienie do przebywania w obszarze przetwarzania - 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 Osobowych, 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 się osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Administrator Danych Osobowych 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 o nazwie: **Gmina Tczów** 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(am) karany(a) za umyślne przestępstwo,
- posiadam pełną zdolność do czynności prawnych, oraz korzystam z pełni praw publicznych,
- posiadam odpowiednią wiedzę z zakresu ochrony danych osobowych.

Administrator Danych Osobowych | **Administrator Bezpieczeństwa Informacji**

..... | .....

Podpis | **Podpis**

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Załącznik 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 (NP. ADRES SIEDZIBY FIRMY GDZIE PRZETWARZANE SĄ DANE)	DZIAŁ UŻYTKUJĄCY POMIESZCZENIE	NR POKOJU LUB POMIESZCZENIA	RODZAJ ZASTOSOWANEGO ZABEZPIECZENIA POMIESZCZENIA	UWAGI
1.	Gmina Tczów Tczów 124, 26-706	Gabinet Wójta	12	✓ Drzwi zamykane na klucz ✓ Szafy zamykane na klucz ✓ Alarm	Brak
		Sekretarz Gminy	12		
		Skarbnik Gminy	15		
		Sekretariat	12		
		Kierownik Referatu Finansów	17		
		Stanowisko pracy ds. księgowości budżetowej	16		
		Stanowisko pracy ds. księgowości podatkowej	13		
		Stanowisko pracy ds. podatków i opłat lokalnych	13		
		Stanowisko pracy ds. rozliczeń opłat za pobór wody, ścieków i odpadów komunalnych	18		
		Stanowisko ds. kasy	14		
		Stanowisko pracy ds. ochrony środowiska i gospodarki nieruchomościami	22		

LP.	DOKŁADNY ADRES (NP. ADRES SIEDZIBY FIRMY GDZIE PRZETWARZANE SĄ DANE)	DZIAŁ UŻYTKUJĄCY POMIESZCZENIE	NR POKOJU LUB POMIESZCZENIA	RODZAJ ZASTOSOWANEGO ZABEZPIECZENIA POMIESZCZENIA	UWAGI
		Stanowisko pracy ds. zamówień publicznych, inwestycji dróg	22		
		Kierownik Referatu Organizacyjnego	24		
		Stanowisko pracy ds. oświaty	24		
		Stanowisko pracy ds. działalności gospodarczej, wojskowych, OC i kancelarii tajnej	11		
		Stanowisko pracy ds. kadr i płac	24		
		Kierownik USC	25		

Data i podpis Administratora Danych Osobowych

.....

ZAŁĄCZNIK NR 3 DO POLITYKI BEZPIECZEŃSTWA:

- **WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH** zgodnie z § 4 pkt 2 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004
- **OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI ORAZ SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI** zgodnie, z § 4 pkt 3 i 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

LP.	NAZWA ZBIORU DANYCH (np. dane klientów, pracowników itd.)	PROGRAMY ZASTOSOWANE DO PRZETWARZANIA DANYCH (np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)	STRUKTURA ZBIORÓW (np. imię i nazwisko, e-mail, telefon itd.)	PRZEPŁYW DANYCH (wersja papierowa ←→ wersja elektroniczna)	UWAGI
1.	**TECZKI AKT OSOBOWYCH PRACOWNIKÓW URZĘDU GMINY**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **KADRY OPTIVUM**	IMIĘ I NAZWISKO, DATA URODZENIA SERIA I NR DOWODU OSOBISTEGO, PESEL, WYKSZTAŁCENIE, ZAŚWIADCZENIA, OŚWIADCZENIA, UPOWAŻNIENIA,	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
2.	**ARKUSZE ORGANIZACYJNE PLACÓWEK OŚWIATOWYCH**	WERSJA TRADYCYJNA (PAPIEROWA)	NAZWISKO, IMIĘ, DATA URODZENIA, PESEL, MIEJSCE PRACY, ZAWÓD, WYKSZTAŁCENIE	WERSJA PAPIEROWA	
3.	**DANE OSOBOWE PRAKTYKANTÓW**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ I NAZWISKO, DATA URODZENIA SERIA I NR DOWODU OSOBISTEGO, PESEL, WYKSZTAŁCENIE	WERSJA PAPIEROWA	
4.	**DANE OSOBOWE STAŻYSTÓW**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ I NAZWISKO, DATA URODZENIA SERIA I NR DOWODU OSOBISTEGO, PESEL, WYKSZTAŁCENIE	WERSJA PAPIEROWA	
5.	**ROZLICZENIE Z URZĘDEM SKARBOWYM Z TYTUŁU PODATKU DOCHODOWEGO OD OSÓB FIZYCZNYCH**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **CENTRALNY REJESTR VAT DLA JST**	IMIĘ I NAZWISKO, ADRES, PESEL, DATA URODZENIA, OBYWATELSTWO, KWOTY PODATKU	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
6.	**DOKUMENTY ROZLICZENIA ZUS**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **PŁATNIK**	IMIĘ I NAZWISKO, ADRES, PESEL, DATA URODZENIA, NAZWISKO RODOWE, OBYWATELSTWO, IMIĘ I NAZWISKO DZIECI, PESEL, DATA URODZENIA, ADRES ZAMIESZKANIA, KWOTY SKŁADEK	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	

LP.	NAZWA ZBIORU DANYCH (np. dane klientów, pracowników itd.)	PROGRAMY ZASTOSOWANE DO PRZETWARZANIA DANYCH (np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)	STRUKTURA ZBIORÓW (np. imię i nazwisko, e-mail, telefon itd.)	PRZEPŁYW DANYCH (wersja papierowa ←→ wersja elektroniczna)	UWAGI
7.	**DZIAŁALNOŚĆ GOSPODARCZA**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIE, ADRES ZAMIESZKANIA LUB POBYTU, PESEL, MIEJSCE PRACY	WERSJA PAPIEROWA	
8.	**ZEZWOLENIA NA SPRZEDAŻ ALKOHOLI**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, NUMER TELEFONU	WERSJA PAPIEROWA	
9.	**AKTA STANU CYWILNEGO**	WERSJA TRADYCYJNA (PAPIEROWA)	NAZWISKO, IMIĘ, IMIONA RODZICÓW, DATA URODZENIA, MIEJSCE URODZENIA, ADRES ZAMIESZKANIA LUB POBYTU, , PESEL, WYKSZTAŁCENIE, SERIA I NR DOWODU OSOBISTEGO, NAZWISKO PANIEŃSKIE, PŁEĆ, STAN CYWILNY, NAZWISKO I IMIĘ WSPÓŁMAŁŻONKA, NUMER AKTU URODZENIA/MAŁŻEŃSTWA, DATA/MIEJSCE/PRZYCZYNA ZGONU, NUMER AKTU ZGONU	WERSJA PAPIEROWA	
10.	**AWANS ZAWODOWY NAUCZYCIELI**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, DATA URODZENIA, MIEJSCE URODZENIA, MIEJSCE PRACY, WYKSZTAŁCENIE	WERSJA PAPIEROWA	
11.	**REJESTR BYŁYCH MIESZKAŃCÓW GMINY**	WERSJA TRADYCYJNA (PAPIEROWA)	NAZWISKO, IMIĘ, IMIONA RODZICÓW, DATA URODZENIA, MIEJSCE URODZENIA, ADRES ZAMIESZKANIA LUB POBYTU, , PESEL, SERIA I NUMER DOWODU OSOBISTEGO, NAZWISKA RODOWE RODZICÓW, NUMER AKTU URODZENIA, NUMER AKTU MAŁŻEŃSTWA, NAZWISKA RODOWE, NUMER AKTU ZGONU	WERSJA PAPIEROWA	
12.	**KURIERZY AKCJI KURIERSKIEJ**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, IMIONA RODZICÓW, DATA URODZENIA, ADRES ZAMIESZKANIA LUB POBYTU, PESEL, MIEJSCE PRACY	WERSJA PAPIEROWA	
13.	**REJESTR DECYZJI O PODZIALE NIERUCHOMOŚCI**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, ADRES ZAMIESZKANIA LUB POBYTU, NR TELEFONU	WERSJA PAPIEROWA	

LP.	NAZWA ZBIORU DANYCH (np. dane klientów, pracowników itd.)	PROGRAMY ZASTOSOWANE DO PRZETWARZANIA DANYCH (np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)	STRUKTURA ZBIORÓW (np. imię i nazwisko, e-mail, telefon itd.)	PRZEPŁYW DANYCH (wersja papierowa ←→ wersja elektroniczna)	UWAGI
14.	**REJESTR DECYZJI O SRODOWISKOWYCH UWARUNKOWANIACH ZGODY NA REALIZACJE PRZEDSIĘWZIĘCIA**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, ADRES ZAMIESZKANIA LUB POBYTU, PESEL, SERIA I NUMER DOWODU OSOBISTEGO, NUMER TELEFONU, DANE DOTYCZĄCE NIERUCHOMOŚCI	WERSJA PAPIEROWA	
15.	**REJESTR DECYZJI O USTALENIE LOKALIZACJI CELU PUBLICZNEGO**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, ADRES ZAMIESZKANIA LUB POBYTU, NR TELEFONU	WERSJA PAPIEROWA	
16.	**REJESTR DECYZJI O WARUNKACH ZABUDOWY TERENU**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, ADRES ZAMIESZKANIA LUB POBYTU, NR TELEFONU	WERSJA PAPIEROWA	
17.	**REJESTR DOKUMENTACJI POWYPADKOWEJ**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ, NAZWISKO, ADRES ZAMMIESZKANIA LUB POBYTU, SERIA I NR DOWODU OSOBISTEGO	WERSJA PAPIEROWA	
18.	**REJESTR EWIDENCJI AZBESTU**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **BAZA AZBESTOWA**	NAZWISKO, IMIĘ, NUMER TELEFONU	WERSJA PAPIEROWA	
19.	**WYKAZ DECYZJI NA USUWANIE DRZEW I KRZEWÓW**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, IMIONA RODZICÓW, DATA URODZENIA, MIEJSCE URODZENIA, ADRES ZAMIESZKANIA LUB POBYTU, , PESEL, NIP, SERIA I NUMER DOWODU OSOBISTEGO	WERSJA PAPIEROWA	
20.	**REJESTR KORESPONDENCJI**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **EZD – ELEKTRONICZNE ZARZĄDZANIE DOKUMENTACJĄ**	NAZWISKO, IMIĘ, ADRES ZAMIESZKANIA LUB POBYTU	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
21.	**REJESTR WYMIAROWY, REJESTR PRZYPISÓW I ODPISÓW**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **MACROLOGIC ERP – PODATEK ROLNY, LEŚNY I OD NIERUCHOMOŚCI I ŚRODKÓW PTRANSPORTU**	NAZWISKO, IMIĘ, IMIONA RODZICÓW, DATA URODZENIA, MIEJSCE URODZENIA, ADRES ZAMIESZKANIA LUB POBYTU, , PESEL, NIP, ADRES NIERUCHOMOŚCI, NAZWISKO RODOWE	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	

LP.	NAZWA ZBIORU DANYCH (np. dane klientów, pracowników itd.)	PROGRAMY ZASTOSOWANE DO PRZETWARZANIA DANYCH (np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)	STRUKTURA ZBIORÓW (np. imię i nazwisko, e-mail, telefon itd.)	PRZEPŁYW DANYCH (wersja papierowa ←→ wersja elektroniczna)	UWAGI
22.	**REJESTR CUDZOZIEMCÓW**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **SELWIN**	NAZWISKO, IMIĘ, IMIONA RODZICÓW, DATA URODZENIA, MIEJSCE URODZENIA, ADRES ZAMIESZKANIA LUB POBYTU, , PESEL, SERIA I NUMER DOWODU OSOBISTEGO, NR I SERIA PASZPORTU, NAZWISKA RODOWE RODZICÓW	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
23.	**REJESTR MIESZKAŃCÓW –GMINA TCZÓW**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **SELWIN**	NAZWISKO, IMIĘ, ADRES ZAMIESZKANIA LUB POBYTU, NR TELEFONU	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
24.	**DOKUMENTY DOTYCZĄCE KONKURSÓW NA DYREKTORÓW SZKÓŁ**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ I NAZWISKO, DATA URODZENIA SERIA I NR DOWODU OSOBISTEGO, PESEL, WYKSZTAŁCENIE, ZAŚWIADCZENIA, OŚWIADCZENIA, UPOWAŻNIENIA	WERSJA PAPIEROWA	
25.	**REJESTR OŚWIADCZEŃ MAJĄTKOWYCH RADNYCH RADY GMINNEJ**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, DATA URODZENIA, ADRES ZAMIESZKANIA LUB POBYTU, MIEJSCE PRACY, DANE DOTYCZĄCE MAJĄTKU OSOBISTEGO	WERSJA PAPIEROWA	
26.	**ORGANIZACJA POBORU**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, DATA URODZENIA, MIEJSCE URODZENIA, ADRES ZAMIESZKANIA LUB POBYTU, PESEL, SERIA I NR DOWODU OSOBISTEGO, NR KSIĄŻECZKI WOJSKOWEJ	WERSJA PAPIEROWA	
27.	**PODATKI I OPŁATY LOKALNE**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **MACROLOGIC ERP – PODATEK ROLNY, LEŚNY I OD NIERUCHOMOŚCI**	NAZWISKO, IMIĘ, IMIONA RODZICÓW, DATA URODZENIA, MIEJSCE URODZENIA, ADRES ZAMIESZKANIA LUB POBYTU, , PESEL, NIP, ADRES NIERUCHOMOŚCI, DANE ADMINISTRATORA NIERUCHOMOŚCI	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
28.	**REJESTR PODATKU OD ŚRODKÓW TRANSPORTU**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **MACROLOGIC ERP – PODATEK OD ŚRODKÓW TRANSPORTOWYCH**	NAZWISKO, IMIĘ, ADRES ZAMIESZKANIA PUB POBYTU, PESEL, NIP, NR REJ POJAZDU	WERSJA PAPIEROWA	
29.	**REJESTR SKARG I WNIOSKÓW**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, ADRES ZAMIESZKANIA LUB POBYTU	WERSJA PAPIEROWA	

LP.	NAZWA ZBIORU DANYCH (np. dane klientów, pracowników itd.)	PROGRAMY ZASTOSOWANE DO PRZETWARZANIA DANYCH (np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)	STRUKTURA ZBIORÓW (np. imię i nazwisko, e-mail, telefon itd.)	PRZEPŁYW DANYCH (wersja papierowa ←→ wersja elektroniczna)	UWAGI
30.	**REJESTR STAŁYCH WYBORCÓW**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **SELWIN**	NAZWISKO, IMIĘ, ADRES ZAMIESZKANIA LUB POBYTU, PESEL	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
31.	**REJESTR UMÓW DZIERŻAWY I NIERUCHOMOŚCI**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, IMIONA RODZICÓW, DATA URODZENIA, MIEJSCE URODZENIA, ADRES ZAMIESZKANIA LUB POBYTU, , PESEL, NIP	WERSJA PAPIEROWA	
32.	**REJESTR WNIOSKÓW O ZEZWOLENIE NA ZAJĘCIE PASA DROGOWEGO**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, ADRES ZAMIESZKANIA LUB POBYTU, NR TELEFONU	WERSJA PAPIEROWA	
33.	**REJESTR WNIOSKÓW POD DZIAŁALNOŚĆ GOSPODARCZĄ I O NAJEM LOKALI UŻYTKOWYCH**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, ADRES ZAMIESZKANIA LUB POBYTU, NIP, NR TELEFONU	WERSJA PAPIEROWA	
34.	**EWIDENCJA ZWROTU PODATKU AKCYZOWEGO**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **MACROLOGIC ERP – PODATEK ROLNY, LEŚNY I OD NIERUCHOMOŚCI**	NAZWISKO, IMIE, ADRES ZAMIESZKANIA LUB POBYTU, PESEL, NIP, SERIA I NR DOWODU OSOBISTEGO	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
35.	**REJESTR WYPADKÓW PRZY PRACY**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ, NAZWISKO, ADRES ZAMMIESZKANIA LUB POBYTU, SERIA I NR DOWODU OSOBISTEGO	WERSJA PAPIEROWA	
36.	**REJESTR ZAPYTAŃ W TRYBIE DOSTĘPU DO INFORMACJI PUBLICZNEJ**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, ADRES ZAMIESZKANIA LUB POBYTU,	WERSJA PAPIEROWA	
37.	**LISTY PŁAC PRACOWNIKÓW URZĘDU**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **KADRY OPTIMUM**	IMIĘ I NAZWISKO, ADRES, PESEL, DATA URODZENIA, NAZWISKO RODOWE, OBYWATELSTWO, IMIĘ I NAZWISKO DZIECI, PESEL, DATA URODZENIA, ADRES ZAMIESZKANIA, KWOTY SKŁADEK	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	

LP.	NAZWA ZBIORU DANYCH (np. dane klientów, pracowników itd.)	PROGRAMY ZASTOSOWANE DO PRZETWARZANIA DANYCH (np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)	STRUKTURA ZBIORÓW (np. imię i nazwisko, e-mail, telefon itd.)	PRZEPŁYW DANYCH (wersja papierowa ←→ wersja elektroniczna)	UWAGI
38.	**SYSTEM INFORMACJI OŚWIATOWEJ**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY: **SIO**	PESEL, MIEJSCE PRACY, ZAWÓD, WYKSZTAŁCENIE, WYSOKOŚĆ WYNAGRODZENIA	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
39.	**UMOWY CYWILNOPRAWNE**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ, NAZWISKO, ADRES, PESEL, NIP, NR KONTA	WERSJA PAPIEROWA	
40.	**ZAMÓWIENIA PUBLICZNE**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, ADRES ZAMIESZKANIA LUB POBYTU, NIP, TELEFON, DANE Z KRS ORAZ CEIDG	WERSJA PAPIEROWA	
41.	**ZESPÓŁ INTERDYSCYPLINARNY**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, DATA URODZENIA, MIEJSCE URODZENIA, ADRES ZAMIESZKANIA LUB POBYTU, PESEL, MIEJSCE PRACY, ZAWÓD, WYKSZTAŁCENIE, SERIA I NR DOWODU OSOBISTEGO, NUMER TELEFONU	WERSJA PAPIEROWA	
42.	**OŚWIADCZENIA MAJĄTKOWE PRACOWNIKÓW URZĘDU**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, DATA URODZENIA, MIEJSCE URODZENIA, ADRES ZAMIESZKANIA LUB POBYTU, MIEJSCE PRACY, ZAWÓD, DANE DOTYCZĄCE MAJĄTKU OSOBISTEGO	WERSJA PAPIEROWA	
43.	**SZKOLENIA STRAŻACKIE**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	NAZWISKO, IMIĘ, DATA URODZENIA, ADRES ZAMIESZKANIA LUB POBYTU	WERSJA PAPIEROWA	
44.	**AKTA OSOBOWE NAUCZYCIELI**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY : **KADRY OPTIMUM**	IMIĘ, NAZWISKO, DATA URODZENIA, SERIA I NR DOWODU OSOBISTEGO, PESEL, WYKSZTAŁCENIE, ZAŚWIADCZENIA, OŚWIADCZENIA, UPOWAŻNIENIA	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
45.	**POMOC ZDROWOTNA NAUCZYCIELI**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY : **KADRY OPTIMUM**	IMIĘ, NAZWISKO, DATA URODZENIA, SERIA I NR DOWODU OSOBISTEGO, PESEL, ADRES ZAMIESZKANIA LUB ZAMELDOWANIA	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	

LP.	NAZWA ZBIORU DANYCH (np. dane klientów, pracowników itd.)	PROGRAMY ZASTOSOWANE DO PRZETWARZANIA DANYCH (np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)	STRUKTURA ZBIORÓW (np. imię i nazwisko, e-mail, telefon itd.)	PRZEPŁYW DANYCH (wersja papierowa ←→ wersja elektroniczna)	UWAGI
46.	**REJESTR ODBIORCÓW WODY**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZNY : **SYSTEM ROZLICZANIA ODBIORCÓW ZA MEDIA KOMUNALNE**	IMIĘ , NAZWISKO, ADRES ZAMIESZKANIA LUB ZAMELDOWANIA, NR DOWODU OSOBISTEGO	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	
47.	**EWIDENCJA WYDANYCH ZAŚWIADCZEŃ DOTYCZĄCYCH GOSPODARSTWA ROLNEGO**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ I NAZWISKO, ADRES ZAMIESZKANIA – ZAMELDOWANIA	WERSJA PAPIEROWA	
48.	**REJESTR UMÓW NA WYNAJEM LOKALI MIESZKALNYCH**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ I NAZWISKO, ADRES ZAMIESZKANIA – ZAMELDOWANIA, PESEL	WERSJA PAPIEROWA	
49.	**REJESTR OSÓB ZGŁOSZONYCH DO GMINNEJ KOMISJI ROZWIĄZYWANIA PROBLEMÓW ALKOHOLOWYCH**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE	IMIĘ I NAZWISKO, ADRES ZAMIESZKANIA – ZAMELDOWANIA, NR DOWODU OSOBISTEGO	WERSJA PAPIEROWA	
50.	**REJESTR CZYTELNIKÓW KORZYSTAJĄCYCH Z GMINNEJ BIBLIOTEKI**	WERSJA TRADYCYJNA (PAPIEROWA) Z WYKORZYSTANIEM PROGRAMU BIUROWEGO TYPU OFFICE + PROGRAM SPECJALISTYCZY: **„KASIA" i „MATEUSZ"**	IMIĘ I NAZWISKO, ADRES ZAMIESZKANIA- ZAMELDOWANIA, NR DOWODU OSOBISTEGO, DATA URODZENIA, NUMER TELEFONU, PESEL, IMIĘ OJCA	WERSJA PAPIEROWA <-- --> WERSJA ELEKTRONICZNA	

Data i podpis Administratora Danych Osobowych

.....

ZGODA NA PRZEBYWANIE
W OBSZARZE PRZETWARZANIA DANYCH

Załącznik nr 4 do Polityki Bezpieczeństwa

Na podstawie zapisów 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 z późn. zm.), a także na podstawie zapisów ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2016r. poz. 922 z późn. zm.):

DATA NADANIA ZGODY: ***30-06-2017r***

ADMINISTRATOR DANYCH OSOBOWYCH: ***Gmina Tczów***

O NUMERZE NIP: ***811-17-14-505***

W OSOBIE: ***Andrzej Wolszczak***

wyraża zgodę Pani/Panu:

IMIĘ I NAZWISKO: ***[IMIĘ I NAZWISKO]***

PESEL: ***[NR PESEL]***

STANOWISKO SŁUŻBOWE: ***[STANOWISKO SŁUŻBOWE]***

CZAS TRWANIA ZGODY: ***DO USTANIA STOSUNKU PRACY***

na przebywanie w pomieszczeniach, w których przetwarzane są dane osobowe w zakresie niezbędnym do wykonywania obowiązków służbowych. Jednocześnie zobowiązuję ww. osobę do zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w pomieszczeniach, co do których uzyskał (a) zgodę na przebywanie.

Zobowiązuję się do zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w pomieszczeniach, co do których uzyskałem (am) zgodę na przebywanie.	
..... (data i podpis osoby upoważnionej do przebywania w obszarze przetwarzania danych)	..... (data, podpis i pieczęć Administratora Danych Osobowych)

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.

Administrator Danych Osobowych – **Gmina Tczów**
w osobie: **Andrzej Wolszczak**
dnia **30-06-2017r** nadaje upoważnienie do przetwarzania danych osobowych, dla:

IMIĘ I NAZWISKO: .....

NR PESEL: .....

STANOWISKO SŁUŻBOWE: .....

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

ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z:

- **POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH**
- **ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY**

Upoważnienie nadaje się do ustania stosunku pracy. Wszelakie poprzednie upoważnienia do przetwarzania danych osobowych z dniem wprowadzenia niniejszego wygasają. Jednocześnie bieżące upoważnienie zostaje zawieszone w przypadku nieobecności / urlopu przekraczającego 30 dni kalendarzowych. Po upływie w/w okresu nieobecności / urlopu upoważniony(a) wykonując obowiązki wynikające z upoważnienia otrzymuje ponowne upoważnienie niniejszym dokumentem w trybie automatycznym.

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

Przyjąłem do wiadomości, iż jestem zobligowany do zmiany hasła dostępu do stanowiska pracy (komputera) w terminie co 30 dni kalendarzowych. Hasło musi być niepowtarzalne względem wcześniejszego, oraz składać się z 8 znaków (w tym małe, duże litery oraz znak specjalny np.: „**REF#gospodarka**" ; „**Kardex2015**" itd...).

Oświadczam, iż zapoznałem(am) się i akceptuję zasady dotyczące korzystania z sieci informatycznej na terenie w/w podmiotu, a mianowicie:

1. Mając na uwadze wysoką sprawność oraz elastyczność kształtowania procesów w pracy, pracodawca zastrzega sobie prawo do archiwizacji, monitorowania oraz przekierowywania służbowej poczty elektronicznej.
2. Pracodawca informuje, że wszystkie połączenia internetowe wykonane w sieci w/w podmiotu są rejestrowane, zgodnie z wymogami ustawy Prawa Telekomunikacyjnego.
3. Pracodawca zastrzega sobie również prawo monitorowania w/w połączeń oraz żądania wyjaśnień w zakresie realizowanej przez pracownika aktywności w sieci oraz do dowolnego kształtowania zakresu dostępu do sieci internetowej.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2016r. 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.

....
[czytelny podpis Administratora Danych Osobowych] [czytelny podpis upoważnionego]

EWIDENCJA OSÓB POSIADAJĄCYCH UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH ORAZ PRZEBYWANIA W OBSZARZE PRZETWARZANIA

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

* (z uwzględnieniem osób nieprzetwarzających dane osobowe, ale przebywających w pomieszczeniach, w których zachodzi proces przetwarzania danych osobowych)

LP.	IMIĘ I NAZWISKO	STANOWISKO SŁUŻBOWE	RODZAJ UPOWAŻNIENIA (PRZETWARZANIE / PRZEBYWANIE)	DATA NADANIA UPOWAŻNIENIA	DATA USTANIA UPOWAŻNIENIA	WYKAZ ZBIORÓW DANYCH WYNIKAJĄCYCH Z UPOWAŻNIENIA	IDENTYFIKATOR (JEŻELI DANE SĄ PRZETWARZANE W SYSTEMIE INFORMATYCZNYM)
1.					DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	
2.					DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	
3.					DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	
4.					DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	
5.					DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	
6.					DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	

LP.	IMIĘ I NAZWISKO	STANOWISKO SŁUŻBOWE	RODZAJ UPOWAŻNIENIA (PRZETWARZANIE / PRZEBYWANIE)	DATA NADANIA UPOWAŻNIENIA	DATA USTANIA UPOWAŻNIENIA	WYKAZ ZBIORÓW DANYCH WYNIKAJĄCYCH Z UPOWAŻNIENIA	IDENTYFIKATOR (JEŻELI DANE SĄ PRZETWARZANE W SYSTEMIE INFORMATYCZNYM)
7.					DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	
8.					DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	
9.					DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	
10.					DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	
11.					DO USTANIA STOSUNKU PRACY	ZBIORY DANYCH OSOBOWYCH WYNIKAJĄCE Z POSIADANYCH UPRAWNIEŃ SPECJALISTYCZNYCH ORAZ ZAKRESU OBOWIĄZKÓW WYNIKAJĄCYCH Z NAWIĄZANEGO STOSUNKU PRACY	

ADMINISTRATOR DANYCH OSOBOWYCH

.....

(data i czytelny podpis Administratora Danych Osobowych)

ZESTAWIENIE DANYCH OSOBOWYCH Z INFORMACJĄ KIEDY I PRZEZ KOGO ZOSTAŁY DO ZBIORU WPROWADZONE ORAZ KOMU SĄ PRZEKAZYWANE

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

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.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					

ADMINISTRATOR DANYCH OSOBOWYCH

.....

(czytelny podpis Administratora Danych Osobowych)

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

Załącznik do „Polityki Bezpieczeństwa" nr 8 zgodnie z § 4 pkt 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.

2. ABI wraz z wyznaczonymi Użytkownikami przeprowadzają okresową analizę ryzyka dla systemu i na tej podstawie przedstawiają Administratorowi Danych propozycje dotyczące zastosowania środków technicznych i organizacyjnych (środków ochrony), celem zapewnienia właściwej ochrony przetwarzanych danych.

3. Określenia poziomu bezpieczeństwa systemu informatycznego dokonuje ABI.

4. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.

5. Środki ochrony, zastosowane przez ABI dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych, obejmują:
   - środki ochrony fizycznej (np. drzwi ochronne, firma ochroniarska, monitoring);
   - środki techniczne (np. firewall, antywirus, podtrzymanie zasilania UPS);
   - środki organizacyjne (np. powołanie ABI, utworzenie Instrukcji zarządzania systemem informatycznym);

6. Zastosowane środki:

ŚRODKI OCHRONY FIZYCZNEJ DANYCH:

a) Zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nieprzeciwpożarowymi).

b) Pomieszczenia, w których przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.

c) Zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętej niemetalowej szafie.

d) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej niemetalowej szafie.

e) Pomieszczenie, w którym przetwarzane są zbiory danych osobowych, zabezpieczone jest przed skutkami pożaru za pomocą wolnostojącej gaśnicy.

f) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

7. **ŚRODKI OCHRONY TECHNICZNEJ DANYCH:**

a) Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.

b) Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.

c) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

d) Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.

e) Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.

f) Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.

g) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.

h) Użyto system Firewall do ochrony dostępu do sieci komputerowej.

i) Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

j) Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.

k) Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.

l) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

m) Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.

n) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.

o) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

8. ŚRODKI ORGANIZACYJNE:

a) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.

b) Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.

c) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.

d) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy oraz Ustawy o ochronie danych osobowych.
W odniesieniu do innych osób upoważnionych do przetwarzania danych osobowych, w sytuacji naruszeń obowiązków wynikających z niniejszego dokumentu ponieść mogą odpowiedzialność odszkodowawczą. Wszystkie osoby upoważnione do przetwarzania danych osobowych mogę ponieść odpowiedzialność karną w sytuacji naruszenia zasad określonych w niniejszym dokumencie.

ADMINISTRATOR DANYCH OSOBOWYCH

.....

(data i czytelny podpis Administratora Danych Osobowych)

DOKUMENT WZORCOWY

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH NR .....

Załącznik do umowy Nr .....

Zawarta w dniu ..... r. w ..... pomiędzy:

[NAZWA INSTYTUCJI ORAZ ADRES]

zwanym w dalszej części niniejszej umowy „**Zleceniodawcą**"

reprezentowanym przez:

[IMIĘ I NAZWISKO]

.....

a

[NAZWA INSTYTUCJI ORAZ ADRES]

zwanym w dalszej części niniejszej umowy „**Wykonawcą**"

reprezentowanym przez:

[IMIĘ I NAZWISKO]

.....

o następującej treści:

§ 1

POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. W związku z realizacją umowy nr ..... z dnia **[DATA]** r. pomiędzy **[PEŁNA NAZWA ZLECENIODAWCY]** a **[PEŁNA NAZWA WYKONAWCY]** ,o **[NAZWA ŚWIADCZONEJ USŁUGI]**. **Zleceniodawca** powierza **Wykonawcy** trybie art. 31 ustawy z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz. U. z 2016 r. poz. 922 z późn. zm) zwanej dalej ,,ustawą" przetwarzanie danych osobowych.
2. **Zleceniodawca** oświadcza, że jest Administratorem Danych, które powierza.
3. Powierzone dane zawierają informacje typu: **[NP. DANE PRACOWNICZE]**.
4. **Zleceniodawca** powierza **Wykonawcy** przetwarzanie danych osobowych w zakresie określonym w § 2.

§ 2

ZAKRES I CEL PRZETWARZANIA DANYCH

1. **Wykonawca** będzie przetwarzał, powierzone na podstawie niniejszej Umowy, następujące kategorie danych osobowych/zbiory danych osobowych/:
   a) imię i nazwisko,
   b) numer ewidencyjny PESEL,
   c) seria i numer dowodu osobistego,
   d) ..... .
2. Celem przetwarzania danych jest **[NP. REALIZACJA OBSŁUGI KADROWO-PŁACOWEJ]**.
3. Zakres przetwarzania obejmuje: **wprowadzanie, wgląd, modyfikację, drukowanie, usuwanie, archiwizację, przesyłanie** (1) danych osobowych.
4. Powierzone przez **Zleceniodawcę** dane osobowe będą przetwarzane przez **Wykonawcę** wyłącznie w celu wykonywania przez **Wykonawcę** na rzecz **Zleceniodawcy** usług szczegółowo opisanych w umowie, o której mowa w § 1 ust.1 i w sposób zgodny z niniejszą Umową.

§ 3

SPOSÓB WYKONANIA UMOWY W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

1. **Wykonawca** zobowiązuje się, przy przetwarzaniu danych osobowych, o których mowa w § 2 ust 1, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych, o których mowa w art. 36 – 39a ustawy.
2. **Wykonawca** oświadcza, że 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 informacyjne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024):
   a) prowadzi dokumentację opisującą sposób przetwarzania danych osobowych,
   b) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zapewniają określony w Rozporządzeniu poziom bezpieczeństwa,

(1) **niepotrzebne wykasować**

c) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem, w zakresie, za który odpowiada Wykonawca,

d) do wykonania czynności objętych umową dopuszcza jedynie osoby posiadające imienne upoważnienia wraz z klauzulą poufności i posiadające odpowiednią wiedzę z zakresu ochrony danych osobowych.

3. **Wykonawca** zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, ustawą oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

4. **Wykonawca** zobowiązuje się niezwłocznie zawiadomić **Zleceniodawcę** o:

   a) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba że zakaz zawiadomienia wynika z przepisów prawa, a w szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienia poufności wszczętego dochodzenia,

   b) każdym nieupoważnionym dostępie do danych osobowych,

   c) każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.

5. **Zleceniodawca** ma prawo do kontroli sposobu wykonywania niniejszej Umowy poprzez przeprowadzenie zapowiedzianych na 7 dni kalendarzowych wcześniej doraźnych kontroli dotyczących przetwarzania danych osobowych przez **Wykonawcę**, oraz żądania składania przez niego pisemnych wyjaśnień.

6. Na zakończenie kontroli, o których mowa w ust. 8, przedstawiciel **Zleceniodawcy** sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron. **Wykonawca** może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez strony.

7. **Wykonawca** zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.

8. **Wykonawca** zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie **Zleceniodawcy** dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.

9. **Wykonawca** może „pod powierzyć" usługi objęte umową, o której mowa w § 1 ust. 1 i niniejszą umową podwykonawcom jedynie za zgodą **Zleceniodawcy**.

§ 4

ODPOWIEDZIALNOŚĆ WYKONAWCY

1. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie, ujawnienie, przekazanie osobom nieupoważnionym.

2. W przypadku naruszenia przepisów ustawy lub niniejszej Umowy z przyczyn leżących po stronie Wykonawcy, w następstwie, czego Zleceniodawca, jako administrator danych osobowych zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Wykonawca zobowiązuje się pokryć Zleceniodawcy poniesione z tego tytułu straty i koszty.

§ 5

CZAS OBOWIĄZYWANIA UMOWY POWIERZENIA

1. Niniejsza Umowa powierzenia zostaje zawarta na czas określony:
   - od dnia **[DATA]** do dnia **[DATA]**.

§ 6

WARUNKI WYPOWIEDZENIA I ROZWIĄZANIA UMOWY

1. **Zleceniodawca** ma prawo rozwiązać niniejszą Umowę bez zachowania terminu wypowiedzenia, gdy **Wykonawca**:
   a) wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową,
   b) powierzył przetwarzanie danych osobowych podwykonawcom bez zgody **Zleceniodawcy**,
   c) nie zaprzestanie niewłaściwego przetwarzania danych osobowych,
   d) zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej Umowy, a w szczególności niespełniania wymagań określonych w §3.

2. Rozwiązanie niniejszej Umowy przez **Zleceniodawcę** jest równoznaczne z wypowiedzeniem umowy, o której mowa w § 1 ust. 1.

3. **Wykonawca**, w przypadku wygaśnięcia umowy, o której mowa §1 ust.1 niniejszej umowy niezwłocznie, ale nie później niż w terminie do 5 dni kalendarzowych, zobowiązuje się zwrócić lub usunąć wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym skutecznie usunąć je również z nośników elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazanym **Zleceniodawcy** protokołem.

§8

POSTANOWIENIA KOŃCOWE

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy Kodeksu cywilnego.
3. Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby **Zleceniodawcy**.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

.....	.....
za Zleceniodawcę	za Wykonawcę

KLAUZULA POUFNOŚCI INFORMACJI

§ 1

Strony umowy zobowiązują się wzajemnie do nie wykorzystywania, nie ujawniania oraz nie przekazywania informacji, które stanowią tajemnicę przedsiębiorstwa drugiej strony niniejszej umowy.

§ 2

Strony powinny zachować poufność informacji, które zdobędą na każdym etapie jakiejkolwiek wzajemnej współpracy.

§ 3

Klauzula poufności danych obowiązuje strony przez okres trwania umowy, a także bezwzględnie po jej zakończeniu przez okres ..... lat.

§ 4

Strony odpowiadają za zachowanie powyższych informacji w tajemnicy przez osoby, którym wykonanie swoich obowiązków powierzyły.

§ 5

Strony umowy zobowiązują się do wykorzystywania przetwarzanych przez nie danych osobowych, w ramach realizacji niniejszej umowy, wyłącznie w celach określonych w umowie.

§ 6

Stronom umowy przysługuje każdym czasie i bez ograniczenia kontrola procesu przetwarzania i ochrony danych osobowych.

§ 7

Strony, dopełniając czynności wynikających z niniejszej umowy, zobowiązują się do przestrzegania przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016r. poz. 922 z późn. zm.)

§ 8

W przypadku nie dochowania warunków umowy, strony zastrzegają sobie prawo rozwiązania niniejszej umowy w trybie natychmiastowym, w każdym czasie.

TREŚĆ OBOWIĄZKU INFORMACYJNEGO ADMINISTRATORA DANYCH OSOBOWYCH

Gmina Tczów
26-706, Tczów 124

reprezentowanym przez:

Andrzej Wolszczak

Zgodnie z art. 24 ust. 1 i art. 25 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 roku poz. 922) informuję, iż administratorem Pani/Pana danych osobowych jest **Gmina Tczów, 26-706 Tczów .** Pani/Pana dane osobowe przetwarzane będą w celu np. przeprowadzenia postępowania rekrutacyjnego na wolne stanowisko pracy np. Młodszy Referent do obsługi sekretariatu. Pana/Pani dane osobowe nie będą udostępniane innym odbiorcom danych za wyjątkiem wypadków obowiązkowego udzielenia informacji określonych w przepisach szczególnych. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania. Podaje Pani/Pan swoje dane osobowe dobrowolnie.

WYJAŚNIENIE CZYM JEST OBOWIĄZEK INFORMACYJNY

Co to jest obowiązek informacyjny?

Obowiązek informacyjny powinien spełniać administrator danych osobowych - w różnych sytuacjach oczywiście. Wynika to wprost z przepisów ustawy o ochronie danych osobowych (podstawowy przepis poniżej):

Art. 24. 1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

1. *adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;*
2. *celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji 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.*

Poza tym, zgodnie z art. 32 ustawy o ochronie danych osobowych (Dz. U. z 2016 roku poz. 922) każdy ma prawo do kontroli przetwarzania danych osobowych tej osoby, której dane dotyczą i może złożyć do administratora danych osobowych zapytanie w formie wniosku o udzielenie informacji, od kiedy dane osobowe są przetwarzane oraz w jakim zakresie.
Ustawa nie określa w jakiej formie obowiązek informacyjny powinien być spełniany: czy w formie ustnej czy pisemnej. Administrator Danych Osobowych powinien, wtedy kiedy to jest wymagane, spełnić ten obowiązek jeszcze przed rozpoczęciem procesu przetwarzania danych.

Obowiązek informacyjny powinien być wypełniany dwutorowo:

- kiedy placówka pobiera dane w innym celu, niż cel wynikający z innych przepisów szczególnych np.: wykonywania zadań publicznych rozumianych wąsko. Przykładem, kiedy obowiązek

informacyjny trzeba będzie spełnić to: rekrutacja na konkretne stanowisko pracy, przeprowadzanie konkursów itd. Konieczność stosowania obowiązku informacyjnego zaistnieje głównie wtedy, kiedy placówka/przedsiębiorstwo będzie musiało pobierać zgodę na przetwarzanie danych osobowych tej konkretnej osoby.

- z drugiej strony obowiązek informacyjny powinien być spełniany w stosunku do osób, które korzystają z uprawnienia wynikającego z art. 32 ustawy o ochronie danych osobowych (Dz. U. z 2016 roku poz. 922) – informacje powyżej.

Przykład wymagalności obowiązku informacyjnego:

Prowadzenie postępowania rekrutacyjnego:

Treść obowiązku informacyjnego powinna znajdować się w zamieszczonej przez jednostkę samorządu terytorialnego, jednostkę organizacyjną samorządu terytorialnego, przedsiębiorstwo - ofercie pracy. Ustawa o ochronie danych osobowych nie narzuca formy spełnienia obowiązku informacyjnego, ale z kolei zobowiązuje do poinformowania w tym trybie przed rozpoczęciem procesu przetwarzania danych osobowych. Ze względów praktycznych należy zamieszczać klauzulę obowiązku informacyjnego w samej treści oferty, podobnie jak informację, że bez klauzuli wyrażenia zgody na przetwarzanie danych osobowych, aplikacje nie będą rozpatrywane. Placówka musi dochować należytej staranności w zakresie czytelności i klarowności treści obowiązku informacyjnego, tak, by treść rzeczywiście nie budziła żadnych wątpliwości. Treść obowiązku informacyjnego powinna być w dostateczny sposób wyodrębniona spośród innych informacji przekazywanych w ofercie potencjalnemu kandydatowi do pracy na stanowisko, co do którego rozpoczyna się procedurę naboru.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

Administrator Danych Osobowych – **Gmina Tczów**
w osobie: **Andrzej Wolszczak** dnia **23-06-2017r**

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 wchodzą w życie z dniem 23-06-2017r .

Ilekroć w „Instrukcji" jest mowa o:

1. **PODMIOCIE** — rozumie się przez to spółkę prawa handlowego, podmiot gospodarczy nieposiadający osobowości prawnej, jednostkę budżetową,
2. **USTAWIE** — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016r. poz. 922 z późn. zm.), 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 35 ustawy z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne (Dz. U. z 2016r., poz. 1489 z późn. zm.),
6. **SIECI PUBLICZNEJ** — rozumie się przez to termin, który przywołuje § 2 ust. 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. (Dz. U. z 2004r. Nr 100, poz. 1024),
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

W podmiocie o nazwie: **Gmina Tczów**, za przestrzeganie zapisów „instrukcji" odpowiedzialny jest **Administrator Danych** lub zgodnie z zapisem §3 „Polityki Bezpieczeństwa" wyznaczony **Administrator Bezpieczeństwa Informacji.**

§ 2

W związku z tym, że w podmiocie o nazwie: **Gmina Tczów** 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 Danych Osobowych. 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: **ESET End Point**,
   - poprzez zainstalowanie firewall (zapora sieciowa),
   - poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem,
2. utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego UPS.

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 na tydzień.

4. Kopie zapasowe:

   a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym: **Serwerownia** , zaopatrzonym w system alarmowy.

   b) usuwa się 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:

   a) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

   b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,

   c) 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:

   a) daty pierwszego wprowadzenia danych do systemu,

   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,

   c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,

   d) 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,

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

2. Odnotowanie informacji, o których mowa w §7 ust. 1 pkt 1,2 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.04.2004r. (Dz. U. z 2004r. Nr 100, poz. 1024), 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 §7 ust. 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.04.2004r. (Dz. U. z 2004r. Nr 100, poz. 1024).

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w §7 ust. 1 pkt. 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29.04.2004r. (Dz. U. z 2004r. Nr 100, poz. 1024), 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 minut, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.

§ 5

Administrator Bezpieczeństwa Informacji, o ile jest wyznaczony, 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.**

Administrator Danych Osobowych

.....

Podpis