ZARZĄDZENIE NR 1/2016

Dyrektora Powiatowego Zarządu Dróg w Świdwinie
z dnia 21 marca 2016 roku
w sprawie ochrony danych osobowych w Powiatowym Zarządzie Dróg w Świdwinie

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2014 r., poz. 1182 ze zm.) oraz § 3 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), zarządzam, co następuje:

§ 1

Wprowadzam następującą dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych w Powiatowym Zarządzie Dróg w Świdwinie:

1. Politykę bezpieczeństwa w zakresie ochrony danych osobowych stanowiącą **załącznik Nr I** do niniejszego zarządzenia,
2. Instrukcję zarządzania systemem informatycznym służącym do przetwarzanych danych osobowych stanowiącą **załącznik Nr II** do niniejszego zarządzenia.

§ 2

Zobowiązuję wszystkich pracowników Powiatowego Zarządu Dróg w Świdwinie (z wyjątkiem zatrudnionych na stanowiskach: robotniczych) do przestrzegania zasad zawartych w niniejszym Zarządzeniu.

§ 3

Z dniem wejścia w życie niniejszego zarządzenia traci moc zarządzenie nr 7/2014 z dnia 8 sierpnia 2014 roku w sprawie ochrony danych osobowych w Powiatowym Zarządzie Dróg w Świdwinie.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Powiatowego Zarządu Dróg
Krzysztof Wasicionek

Załącznik Nr 1
do Zarządzenia Nr 1/2016
z dnia 21.03.2016 r.

POLITYKA BEZPIECZEŃSTWA

W ZAKRESIE W ZAKRESIE OCHRONY DANYCH OSOBOWYCH W POWIATOWYM ZARZĄDZIE DRÓG W ŚWIDWINIE

§ 1.

1. Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Powiatowym Zarządzie Dróg w Świdwinie, 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 papierowych oraz w systemach informatycznych.
2. 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.

§ 2.

Polityka dotyczy wszystkich danych osobowych przetwarzanych w Powiatowym Zarządzie Dróg w Świdwinie, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.

§ 3.

Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych w tym oddziałów, samodzielnych stanowisk pracy i wszystkich procesów przebiegających w ramach przetwarzania danych osobowych

§ 4.

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:

1. zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
3. systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. zabezpieczeniu danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich

nieuprawnionym przetwarzaniem,

5. usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6. Administratorze Danych Osobowych - rozumie się przez to Dyrektora Powiatowego Zarządu w Świdwinie,
7. Administratorze Bezpieczeństwa Informacji – rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych w celu nadzorowania i przestrzegania zasad ochrony, o których mowa w § 1.
8. podmiocie – rozumie się przez to Powiatowy Zarząd Dróg w Świdwinie;

§ 5.

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

§ 6.

1. Obszar przetwarzania danych osobowych stanowią pomieszczenia Powiatowego Zarządu Dróg w Świdwinie, w których wykonywane są operacje na danych osobowych, takie jak ich zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie przy użyciu stacjonarnego sprzętu komputerowego lub w formie kartotek, skorowidzów, ksiąg, wykazów i innych zbiorów ewidencyjnych.
2. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych, w sposób uniemożliwiający dostęp osób trzecich. Osoby postronne mogą przebywać wewnątrz wyżej wymienionego obszaru jedynie w obecności osoby upoważnionej do przetwarzania danych osobowych. W pomieszczeniach, w których przebywają osoby postronne, monitory stanowisk dostępu powinny być ustawione w sposób uniemożliwiający wgląd w dane osobom trzecim.
3. Budynek, w którym zlokalizowany jest obszar przetwarzania danych osobowych, jest chroniony przez elektroniczny system alarmowy nadzorowany przez firmę ochroniarską.
4. Urządzenia służące do przetwarzania danych osobowych znajdują się w zamkniętych pomieszczeniach.
5. Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe określa **załącznik nr 2 do „Polityki Bezpieczeństwa".**

§ 7.

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

§ 8.

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

§ 9.

W Powiatowym Zarządzie Dróg w Świdwinie dba się o to, aby dane osobowe w formie papierowej były niedostępne dla osób nieupoważnionych. Dokumenty znajdują się w pomieszczeniach zamykanych na klucz, do których dostęp mają tylko osoby posiadające aktualne upoważnienie do przetwarzania danych osobowych. Tymczasowe wydruki z danymi osobowymi po ustaniu ich przydatności są niszczone w niszczarkach.

§ 10.

1. Do przetwarzania danych dopuszczone są 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. Administrator Danych Osobowych nadaje uprawnienia pracownikom, którzy przetwarzają dane poprzez podpisanie upoważnienia, które stanowi **załącznik nr 5 do „Polityki Bezpieczeństwa"**.

2. Prowadzona jest dokumentacja opisująca sposób przetwarzania danych w Powiatowym Zarządzie Dróg w Świdwinie, a w szczególności:
   1) Ewidencja osób upoważnionych do przetwarzania danych osobowych w Powiatowym Zarządzie Dróg w Świdwinie – **załącznik nr 6** do „Polityki Bezpieczeństwa".
   2) Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych - **załącznik nr 7 do „Polityki Bezpieczeństwa"**.
3. 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.

§ 11.

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.

§ 12.

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

§ 13.

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

§ 14.

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.

Administrator Danych Osobowych

DYREKTOR
Powiatowego Zarządu Dróg
Krzysztof Wasicionek

WZÓR **załącznik nr 1** do „Polityki Bezpieczeństwa"

.....

miejscowość i data

Upoważnienie dla Administratora Bezpieczeństwa Informacji oraz zakres obowiązków

Na podstawie art. 36a ust. 1 Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz. U. z 2014 r. poz. 1182, 1662)
Administrator Danych Osobowych – Dyrektor Powiatowego Zarządu Dróg w Świdwinie z siedzibą w Świdwinie przy ul. Podmiejskiej 18 NIP: 672-17-28-350 powołuje
Administratora Bezpieczeństwa Informacji *(imię i nazwisko)*..... pesel .....

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

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

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

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

- zgodnie z § 4. „Polityki Bezpieczeństwa":
Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, który określa załącznik do „Polityki Bezpieczeństwa" nr 2,

- zgodnie z § 5. „Polityki Bezpieczeństwa":
Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, który określa załącznik do „Polityki Bezpieczeństwa" nr 3,

- zgodnie z § 6. „Polityki Bezpieczeństwa":
Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, który określa załącznik do „Polityki Bezpieczeństwa" nr 4,

- zgodnie z § 8. „Polityki Bezpieczeństwa":
Ewidencję osób przetwarzających dane w podmiocie posiadających upoważnienie – według załącznika nr 6 do „Polityki Bezpieczeństwa" oraz zestawienie danych osobowych z informacją kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane według załącznika nr 7 do „Polityki Bezpieczeństwa".

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

WZÓR

załącznik nr 1 do „Polityki Bezpieczeństwa"

Administrator Bezpieczeństwa Informacji zapewnia zapoznanie 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 Powiatowym Zarządzie Dróg w Świdwinie 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 karany za umyślne przestępstwo,
- posiadam pełną zdolność do czynności prawnych oraz korzystam z pełni praw publicznych,
- posiadam odpowiednią wiedzę z zakresu ochrony danych osobowych.

Administrator Bezpieczeństwa Informacji

.....
Podpis

Administrator Danych Osobowych

.....
Podpis

załącznik Nr 2 do „Polityki Bezpieczeństwa"

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

Lp.	**Dokładny adres** *(np. adres siedziby firmy gdzie przetwarzane są dane)*	**Dział użytkujący pomieszczenie**	**Nr pokoju lub pomieszczenia**	**Rodzaj zastosowanego zabezpieczenia pomieszczenia**	**Uwagi**

WZÓR

załącznik Nr 3 do „Polityki Bezpieczeństwa"

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

Lp.	**Nazwa zbioru danych** *(np. dane klientów, pracowników itd.)*	**Programy zastosowane do przetwarzania danych** *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	**Uwagi**

WZÓR

załącznik nr 4 do „Polityki Bezpieczeństwa"

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami

Lp.	**Nazwa zbioru danych** *(np. dane klientów, pracowników itd.)*	**Struktura zbiorów** *(np. imię i nazwisko, e-mail, telefon itd.)*	**Przepływ danych** (np. wydruk danych z internetu)	**Uwagi**

WZÓR **załącznik nr 5** do „Polityki Bezpieczeństwa"

Upoważnienie do przetwarzania danych osobowych

nr .....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2002 Nr 101, poz. 926 z późn. zm.) **upoważniam Panią/Pana*** ..... **pracownika Powiatowego Zarządu Dróg w Świdwinie zatrudnionego / zatrudnioną na stanowisku** .....

do wykonywania czynności związanych z przetwarzaniem danych osobowych w zakresie obsługi systemu informatycznego i urządzeń wchodzących w jego skład.

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej (kartoteki, ewidencje, rejestry, spisy itp.) i elektronicznej, wg wykazu zbiorów:

1. .....
2. .....
3. .....
4. .....
5. .....
6. .....

Niniejsze upoważnienie nie upoważnia do udzielania dalszych upoważnień i wygasa z dniem ustania stosunku pracy, a ponadto może być w każdym czasie zmienione lub odwołane.

.....

(data i podpis Administratora Danych Osobowych)

Ja niżej podpisany(a) zobowiązuję się do przestrzegania zasad panujących w Powiatowym Zarządzie Dróg w Świdwinie w zakresie ochrony danych osobowych a w szczególności „Polityki Bezpieczeństwa" i Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.

Zobowiązuję się również do zapewnienia ochrony danych, zachowania tajemnicy dotyczącej danych osobowych przetwarzanych w podmiocie oraz sposobów zabezpieczeń a także zgłaszania faktu naruszenia/zagrożenia zabezpieczeń danych osobowych.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami Ustawy o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182,1662) 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(a) 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.

.....

(data i podpis upoważnionego pracownika)

* Niepotrzebne skreślić

WZÓR

załącznik nr 6 do „Polityki Bezpieczeństwa"

Ewidencja osób
upoważnionych do przetwarzania danych osobowych
w Powiatowym Zarządzie Dróg w Świdwinie

Lp.	Imię i nazwisko	Zbiór danych osobowych	Rodzaj systemu	Data nadania upoważnienia	Data ustania upoważnienia
1					
2					
3					
4					
5					
6					
7					
8					

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

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,
   - środki techniczne,
   - środki organizacyjne.

6. Zastosowane środki ochrony fizycznej pomieszczeń:
   - Główne drzwi wejściowe do budynku, poza godzinami urzędowania Powiatowego Zarządu Dróg w Świdwinie zamykane są na 2 zamki.
   - Wszystkie pomieszczenia biurowe, magazynowe oraz pomieszczenie archiwum wyposażone są w drzwi zamykane na zamek po zakończeniu pracy oraz na czas nieobecności w nich osób zatrudnionych.
   - Budynek, w którym zlokalizowany jest obszar przetwarzania danych osobowych, jest chroniony przez elektroniczny system alarmowy nadzorowany przez Agencję Ochrony.

7. Zastosowane środki techniczne:
   - Systemy operacyjne na komputerach w Powiatowym Zarządzie Dróg w Świdwinie chronione są przez program antywirusowy GDATA Antywirus oraz zaporę sieciową (firewall) COMODO Personal Firewall.
   - Komputery stacjonarne w Powiatowym Zarządzie Dróg w Świdwinie wyposażone są w awaryjne podtrzymanie zasilania za pomocą zasilaczy UPS.
   - Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętej metalowej szafie pancernej.
   - Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek.

8. Zastosowane środki organizacyjne:
   - Zarządzeniem Nr 7/2014 z dnia 8 sierpnia 2014 r. Dyrektora Powiatowego Zarządu Dróg w Świdwinie została wprowadzona dokumentacja przetwarzania danych osobowych, która podlega ewaluacji wynikającej z doświadczeń praktycznych i zmian w przepisach.
   - Zgodnie z art. 36a ust. 1 ustawy o ochronie danych osobowych, Administrator danych powołał Administratora Bezpieczeństwa Informacji, który został zgłoszony do rejestru Generalnego Inspektora Ochrony Danych Osobowych..

- Przetwarzanie danych osobowych w Powiatowym Zarządzie Dróg w Świdwinie może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań.
- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie.
- ABI prowadzi ewidencję osób upoważnionych oraz przygotowuje Upoważnienia do przetwarzania danych i przedkłada je do podpisu Administratorowi Danych Osobowych.

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

Załącznik Nr II
do Zarządzenia Nr 1/2016
z dnia 21.03.2016 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM służącym do przetwarzania danych osobowych w Powiatowym Zarządzie Dróg w Świdwinie

Ilekroć w „instrukcji" jest mowa o:

1) podmiocie — rozumie się przez to Powiatowy Zarząd Dróg w Świdwinie;
2) ustawie — rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwaną dalej „ustawą";
3) identyfikatorze użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
4) haśle — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
5) sieci telekomunikacyjnej — rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
6) sieci publicznej — rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. — Prawo telekomunikacyjne;
7) teletransmisji – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej
8) rozliczalności — rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
9) integralności danych — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) raporcie — rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych;
11) poufności danych — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
12) uwierzytelnianiu — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

§ 1

Za przestrzeganie w Powiatowym Zarządzie Dróg w Świdwinie zapisów „instrukcji" odpowiedzialny jest powołany **Administrator Bezpieczeństwa Informacji.**

§2

W związku z tym, że w Powiatowym Zarządzie Dróg w Świdwinie 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 Osobowych, 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 GDATA Antywirus,
   - poprzez zainstalowanie zapory sieciowej (firewall) COMODO Personal Firewall.
   - 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. Kopie zapasowe baz danych oraz aplikacji bazodanowych zlokalizowanych na stanowiskach komputerowych wykonywane są w cyklu miesięcznym, tworzone „ręcznie", natomiast pełny backup systemu (łącznie z kopią systemu operacyjnego serwera) wykonywany jest w cyklu rocznym, tworzony ręcznie.
4. Kopie zapasowe:
   a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym tj. w szafie pancernej w pokoju nr (Dział Techniczny) zaopatrzonym w kraty w oknach i elektroniczny 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:

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

§3

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:
   1) daty pierwszego wprowadzenia danych do systemu;
   2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1) i 2), następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

§4

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

§5

Administrator Bezpieczeństwa Informacji ma obowiązek dokonywać przeglądów technicznych sprzętu informatycznego w podmiocie oraz dbać o ich dobry stan techniczny. Zaleca się dokonywanie przeglądów okresowych co najmniej raz na kwartał 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

DYREKTOR
Powiatowego Zarządu Dróg
Krzysztof Wasicionek