ZARZĄDZENIE NR 032/2018

Burmistrza Nowego Warpna
z dnia 24 maja 2018 roku

w sprawie wdrożenia Polityk Ochrony Danych Osobowych w Urzędzie Gminy w Nowym Warpnie

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (t. j. DzU z 2018 r. poz. 130) w związku z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dziennik Urzędowy UE - 4.5.2016 L 119/3) **zarządza się, co następuje:**

§ 1.

Wprowadzam w życie w Urzędzie Gminy w Nowym Warpnie (zwany dalej „urzędem") Politykę Ochrony Danych Osobowych, która stanowi załącznik 1 do zarządzenia.

§ 2.

Zadania związane z prawidłowością przetwarzania danych osobowych w urzędzie realizują wszyscy pracownicy zatrudnieni w jednostce, a za skuteczne funkcjonowanie Polityki Ochrony Danych odpowiedzialny jest Burmistrz Nowego Warpna.

§ 3.

Zasady ochrony danych określone są w Regulaminie Ochrony Danych, który stanowi załącznik nr 2 do zarządzenia.

§ 4.

Zobowiązuję wszystkich pracowników do zapoznania się z przepisami ochrony danych, obowiązujących w urzędzie, oraz do złożenia pisemnego oświadczenia o zapoznaniu się z Regulaminem Ochrony Danych w terminie do 25 maja 2018 r. Wzór oświadczenia stanowi załącznik nr 3 i 4 do zarządzenia.

§ 5.

Funkcję Inspektora Ochrony Danych sprawuje Bartosz Kaniuk. Dane do kontaktu: iodo.szczecin@gmail.com, tel. 579 979 237.

§ 6.

Zarządzenie wchodzi w życie z dniem 25 maja 2018 r.

Załącznik nr 1 do Zarządzenia nr 032/2018
Burmistrza Nowego Warpna
Z dnia 24 maja 2018 roku

POLITYKA OCHRONY DANYCH OSOBOWYCH W URZĘDZIE GMINY NOWE WARPNO, PLAC ZWYCIĘSTWA 1

Spis treści

I. NAJWAŻNIEJSZE DEFINICJE/ SŁOWNICZEK POJĘĆ 4

II. ANALIZA RYZYKA (OCENA SKUTKÓW DLA OCHRONY DANYCH) 6

III. DEFINICJE 7

IV. WYZNACZENIE ZAGROŻEŃ 7

V. WYLICZANIE RYZYKA DLA ZAGROŻEŃ 8

VI. REAKCJA NA WARTOŚĆ RYZYKA 9

VII. UPOWAŻNIENIA 9

VIII. ZALECENIA W WYPADKU WYSTĄPIENIA EPIZODÓW, KTÓRE MOGĄ ZAGROZIĆ BEZPIECZEŃSTWU DANYCH OSOBOWYCH 9

IX. REGULAMIN OCHRONY DANYCH OSOBOWYCH 10

X. AUDYTY 10

XI. WYKAZ ZABEZPIECZEŃ 11

Dokument ten opisuje zasady, jakie należy zachować, aby dane osobowe zostały chronione przez Administratora (podmiot, który je przetwarza w celu spełnienia wymagań RODO). Polityka ma za zadanie wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z wymogami Parlamentu Europejskiego i Rady Europy.

I. NAJWAŻNIEJSZE DEFINICJE/ SŁOWNICZEK POJĘĆ

administrator danych osobowych	oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
anonimizacja	zmiana danych osobowych, która oznacza utratę charakteru danych osobowych;
dane biometryczne	oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
dane dotyczące zdrowia	oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia;
dane genetyczne	oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
dane osobowe	oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
incydent bezpieczeństwa danych	może to być zdarzenie losowe zewnętrzne (pożar, zalanie wodą pomieszczenia, utrata zasilania), zdarzenie losowe wewnętrzne (awaria komputera lub serwera, pomyłka informatyka lub samego użytkownika, utrata lub zagubienie danych), umyślne incydenty (kradzież danych lub sprzętu, wyciek informacji, świadome niszczenie dokumentów, działania wirusów i szkodliwego oprogramowania);
inspektor danych osobowych (IOD)	jest osobą, która została formalnie wybrana przez administratora danych osobowych do doradztwa i przekazywania informacji administratorowi, podmiotowi przetwarzającemu dane osobowe oraz

	pracownikom (w zakresie prawa dotyczącego ochrony danych osobowych. Do zadań IOD należy również kontrola i monitorowanie przestrzegania działań w zakresie polityki ochrony danych osobowych. Celem działania inspektora danych osobowych jest również kontakt między osobami przetwarzającymi dane, a organem nadzorczym.
naruszenie ochrony danych osobowych	oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
odbiorca	oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
ograniczenie przetwarzania	oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
podatność bezpieczeństwa danych osobowych	niewłaściwe zabezpieczenie pomieszczeń, urządzeń i dokumentów; niewłaściwe zabezpieczenie sprzętu IT i oprogramowania przed wyciekiem lub kradzieżą danych osobowych; niestosowanie zasad ochrony danych przez pracowników (nieprzestrzeganie zasady czystego biurka, ochrony haseł, niezamykanie szafek i pomieszczeń);
podmiot przetwarzający (procesor)	oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
profilowanie	oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
przetwarzanie danych osobowych	oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
pseudonimizacja	oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
RODO	rozporządzenie Parlamentu Europejskiego i Rady Europy nr 2016/679, które obejmuje sprawy ochrony osób fizycznych, w związku z

	przetwarzaniem danych osobowych;
strona trzecia	oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które - z upoważnienia administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe;
zbiór danych	oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
zgoda osoby, której dane dotyczą	oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

II. ANALIZA RYZYKA (OCENA SKUTKÓW DLA OCHRONY DANYCH)

Jeżeli dany rodzaj przetwarzania danych, może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, należy dokonać oceny skutków planowanych operacji przetwarzania danych. Ocena ta, ma służyć formalnej analizie ryzyka. Za jej wykonanie odpowiada Administrator, przy współudziale Inspektora Danych Osobowych.

A. inwentaryzacja aktywów (operacje przetwarzania i ich opis)

W celu dokonania tej analizy, należy zidentyfikować dane osobowe, które trzeba zabezpieczyć w postaci zbiorów (wykaz zbiorów danych osobowych – zał. nr 1). Opis zbiorów musi zawierać niezbędne informacje w postaci:

- nazwy zbioru,
- opisu celów przetwarzania,
- zakresu i charakteru danych osobowych,
- odbiorców danych osobowych,
- opisu operacji przetwarzania danych osobowych,
- środków, które są niezbędne do przetwarzania danych osobowych, np. programów, systemów operacyjnych, informacji, infrastruktury, pracowników (lista aktywów – zał. nr 2),
- powiadomienia o konieczności wpisu do rejestru czynności przetwarzania oraz konieczności przeprowadzenie oceny skutków dla opisu kategorii osób.

B. zgodność z przepisami RODO (ocena proporcjonalności i niezbędności)

Aby dokonać analizy ryzyka Administrator lub podmiot, który przetwarza dane osobowe, winien jest spełnić obowiązki prawne i formalne wobec nich. Należy zagwarantować to, że:

- dane będą legalnie przetwarzane,
- dane będą odpowiednie w stosunku do celu ich przetwarzania,
- dane będą przetwarzane przez określony czas,

- wobec osób, których dane osobowe będą przetwarzane, zostanie wykonany obowiązek informacyjny, którego celem jest wskazanie praw tych osób. Należy poinformować je, że mają prawo do dostępu do danych, do ich przenoszenia, sprostowania, usunięcia bądź ograniczenia ich przetwarzania, a także do sprzeciwu przetwarzania danych oraz do odwołania zgody na przetwarzanie danych osobowych,
- zostały przygotowane klauzule informacyjne dla osób, których dane osobowe będą przetwarzane (klauzule informacyjne – zał. nr 3)
- zostały przygotowane umowy powierzenia z podmiotami przetwarzającymi dane (umowa powierzenia – zał. nr 4, oraz rejestr umów powierzenia – zał. nr 5).

C. analiza ryzyka, procedura

W celu zabezpieczenia danych osobowych należy przygotować procedurę przeprowadzenia analizy ryzyka. Działanie to musi być odpowiednie do występujących zagrożeń, które mogą wynikać z przypadkowego lub niezgodnego z prawem dostępu do danych osobowych. Zagrożenie to może wynikać także ze zniszczenia, utraty, modyfikacji, lub nieuprawnionego ujawnienia lub nieuprawnionego dostępu do tych danych.

Analizę ryzyka przeprowadza się dla zbioru lub grupy zbiorów, lub dla procesów przetwarzania danych osobowych.

III. DEFINICJE

A ***aktywa***- zasoby materialne i niematerialne, które mają wpływ na przetwarzanie danych osobowych;

B ***przypadek naruszenia ochrony danych osobowych (jednorazowe zdarzenie)***- to naruszenie bezpieczeństwa ochrony danych osobowych, które prowadzi do zniszczenia, utracenia lub zmodyfikowania danych osobowych. Może także wiązać się z ujawnieniem lub nieuprawnionym dostępem do danych osobowych przez osoby trzecie,

C ***ryzyko***- prawdopodobieństwo wystąpienia zagrożenia, które może powodować straty lub zniszczenie zasobów zawierających dane osobowe,

D ***skutki***- efekty niepożądane incydentu (straty w wypadku wystąpienia zagrożenia),

E ***zagrożenie***-potencjalne naruszenie ochrony danych osobowych.

IV. WYZNACZENIE ZAGROŻEŃ

A Administrator odpowiada za określenie listy ryzyk/zagrożeń, mogących wystąpić w przetwarzaniu danych osobowych w zbiorze lub w procesie przetwarzania,

B należy wskazać zagrożenia, w odniesieniu do poprzednio zidentyfikowanych aktywów,

C wykazanie ryzyk i zagrożeń stanowi lista potencjalnych zagrożeń – zał. nr 6.

V. WYLICZANIE RYZYKA DLA ZAGROŻEŃ

A	**P**- prawdopodobieństwo wystąpienia zagrożeń w zbiorze lub procesie przetwarzania danych (określone przez Administratora). Należy wyróżnić 3 poziomy występowania zagrożeń:

Prawdopodobieństwo wystąpienia zagrożenia	Poziom
niskie	1
średnie	2
wysokie	3

B	**S**-skutki wystąpienia ryzyk (urzeczywistnienie zagrożeń). Skutki powinny uwzględniać straty finansowe, utratę reputacji oraz skutki karne.

Skutki wystąpienia zagrożenia	Poziom
małe (do 10000 zł)	1
średnie (1000- 100000 zł)	2
wysokie (od 100000 zł)	3

C	**R**- ryzyka wyliczane przez Administratora dla wszystkich zagrożeń i występujących dla nich skutków. Obliczanie ryzyka wyliczane jest wg formuły

R=P*S

Poziomy ryzyka	Wartość (R= P*S)
akceptowalne	1-2
opcjonalne	3-6
nieakceptowalne	9

VI. REAKCJA NA WARTOŚĆ RYZYKA

A *uznanie ryzyka*- nie ma potrzeby stosowania dodatkowych zabezpieczeń, ponieważ zabezpieczenia są właściwe i odpowiednie,

B *działania mające na celu zredukowanie ryzyka* (Administrator danych osobowych może je zastosować)- **przeniesienie, unikanie i redukcja.** Przeniesienie związane jest z przerzuceniem ryzyka (ubezpieczenie, outsourcing), unikanie ma wykluczyć działania, które powodują ryzyko (zakaz wynoszenia komputerów przenośnych poza obszar jednostki), redukcja ma na celu zastosowanie takich zabezpieczeń, które mają za zadanie obniżyć ryzyko (szyfrowanie przenośnych nośników danych, które są użytkowane poza obszarem jednostki),

C analiza ryzyka przeprowadzane jest w szablonie (arkusz analizy ryzyka RODO – zał. nr 7),

D ponowna analiza ryzyka jest realizowana cyklicznie. Można jej dokonywać również po wprowadzeniu ważnych zmian w przetwarzaniu danych osobowych (zmiana prawa),

E wprowadzenie list zabezpieczeń do wdrożenia, terminów ich realizacji i osób za to odpowiedzialnych, wszędzie tam, gdzie Administrator postanowi obniżyć ryzyko.

VII. UPOWAŻNIENIA

A za nadawanie i anulowanie upoważnień do przetwarzania danych osobowych w zbiorach (papierowych i informatycznych) odpowiada Administrator,

B osoby upoważnione do przetwarzania danych osobowych dokonują tego wyłącznie na polecenie Administratora (lub na podstawie przepisu prawa),

C upoważnienia są nadawane na wniosek przełożonego i określają zakres operacji na tych danych (upoważnienie do przetwarzania danych osobowych – zał. nr 8),

D Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych – zał. nr 9. Celem tego rejestru jest kontrola nad prawidłowym dostępem do danych osób upoważnionych.

VIII. ZALECENIA W WYPADKU WYSTĄPIENIA EPIZODÓW, KTÓRE MOGĄ ZAGROZIĆ BEZPIECZEŃSTWU DANYCH OSOBOWYCH

Procedura ta opisuje sposób postępowania w przypadku incydentów zagrażających bezpieczeństwu. Ma też na celu ograniczenie ryzyka powstawania zagrożeń i występowania incydentów w przyszłości.

A	osoby posiadające upoważnienia do przetwarzania danych osobowych są zobligowane do niezwłocznego poinformowania przełożonego lub IOD, o sytuacji, w której wystąpiło stwierdzenie incydentu,
B	w przypadku wystąpienia incydentu, Administrator (lub IOD) winien przeprowadzić postępowanie wyjaśniające, które ustali przyczyny i zakres niepożądanego zdarzenia, oraz określi jego ewentualne skutki. Administrator (lub IOD) podejmuje działania dyscyplinarne i działa na rzecz przywrócenia sprawnego działania jednostki po wystąpieniu incydentu. Osoba odpowiedzialna za przetwarzanie danych osobowych zaleca działania zapobiegawcze, które mają w przyszłości eliminować wystąpienie podobnych incydentów, lub zmierzają do zmniejszenia strat w momencie ich zaistnienia,
C	wystąpienie incydentów powinno być udokumentowane przez Administratora, w tym wszystkie okoliczności, w których doszło do naruszenia ochrony danych osobowych. Winne być opisane skutki i podjęte działania, dążące do naprawienia zaistniałej sytuacji (formularz rejestracji incydentu – zał. nr 10),
D	administrator powinien zapewnić możliwość do jak najszybszego przywrócenia dostępności danych osobowych, dzięki zastosowaniu procedur przywracania danych,
E	surowo zabronione jest świadome lub nieumyślne wywoływanie incydentów przez osoby upoważnione do przetwarzania danych osobowych,
F	gdy następuję naruszenie danych osobowych skutkujące naruszeniem praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki (nie później niż 72 godziny po wystąpieniu incydentu) powiadamia organ nadzorczy.

IX. REGULAMIN OCHRONY DANYCH OSOBOWYCH

Dokument ten ma na celu zapewnienie niezbędnej wiedzy osobom, które przetwarzają dane osobowe, jak w bezpieczny sposób to robić (regulamin ochrony danych osobowych). Każda osoba, która zapoznała się z tym dokumentem zobowiązana jest do potwierdzenia znajomości tych zasad i deklaracji ich stosowania (oświadczenie poufności).

Każdy nowozatrudniony pracownik powinien być poddany przeszkoleniu i zapoznaniu z przepisami RODO, zanim zostanie dopuszczony do pracy z danymi osobowymi. Za przeprowadzenie szkolenia odpowiedzialny jest Administrator. Po przeprowadzaniu szkolenia wewnętrznego należy udokumentować ten fakt. Uczestnicy po odbyciu szkolenia zobowiązani się podpisania oświadczenia poufności, które potwierdzi znajomość tych zasad i deklarację ich stosowania.

X. AUDYTY

Zgodnie z rozporządzeniem RODO do zadań Administratora należy regularne mierzenie, testowanie i ocena skuteczności środków technicznych i organizacyjnych, które mają zapewnić ochronę i bezpieczeństwo przetwarzania danych osobowych.

XI. WYKAZ ZABEZPIECZEŃ

Administrator sprawuje nadzór i kontrolę nad wykazem zabezpieczeń, który ma na celu ochronę danych osobowych (instrukcja zarządzania systemami informatycznymi – zał. nr 11 oraz wykaz zabezpieczeń RODO – zał. nr 12). Dokumenty te opisują stosowane zabezpieczenia w jednostce i są aktualizowane po każdej analizie ryzyka i ocenie skutków.

Załączniki:

1. wykaz zbiorów danych osobowych
2. lista aktywów
3. klauzule informacyjne
4. umowa powierzenia
5. rejestr umów powierzenia
6. lista potencjalnych zagrożeń
7. arkusz analizy ryzyka RODO
8. upoważnienie do przetwarzania danych osobowych
9. ewidencję osób upoważnionych do przetwarzania danych osobowych
10. formularz rejestracji incydentu
11. instrukcja zarządzania systemami informatycznymi
12. wykaz zabezpieczeń RODO

Załącznik nr 2 do Zarządzenia nr 032/2018
Burmistrza Nowego Warpna
Z dnia 24 maja 2018 roku

REGULAMIN OCHRONY DANYCH OSOBOWYCH W JEDNOSTCE

SPIS TREŚCI

I. REGULAMIN OCHRONY DANYCH OSOBOWYCH 14

II. BEZPIECZNE UŻYTKOWANIE SPRZĘTU IT, PROGRAMÓW I DYSKÓW 14

III. ADMINISTROWANIE UPRAWNIENIAMI- ROZPOCZĘCIE, ZAWIESZENIE I ZAKOŃCZENIE PRACY 15

IV. POLITYKA HASEŁ 15

V. JAK ZABEZPIECZYĆ DOKUMENTACJĘ PAPIEROWĄ Z DANYMI OSOBOWYMI 16

VI. WYNOSZENIE NOŚNIKÓW Z DANYMI POZA JEDNOSTKĘ 16

VII. BEZPIECZNE KORZYSTANIE Z POCZTY ELEKTRONICZNEJ ORAZ OCHRONA ANTYWIRUSOWA 17

VIII. BEZPIECZNE KORZYSTANIE Z INTERNETU 18

IX. JAK POSTĘPOWAĆ, GDY NARUSZONA ZOSTANIE OCHRONA DANYCH OSOBOWYCH 19

X. POUFNOŚĆ I OCHRONA DANYCH OSOBOWYCH 20

XI. CZYNNOŚCI DYSCYPLINARNE 20

I. REGULAMIN OCHRONY DANYCH OSOBOWYCH

REGULAMIN

Regulamin ochrony danych osobowych jest wykazem obowiązków, które wynikają z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO. Obowiązki te dotyczą przede wszystkim: pracowników, współpracowników, innych pracowników, którzy posiadają dostęp do przetwarzanych danych przez Administratora/ jednostkę oraz użytkowników systemów informatycznych którzy posiadają dostęp do przetwarzanych danych przed Administratora/ jednostkę.

Należy zapoznać każdą z tych osób z tym dokumentem, oraz zobowiązać je do stosowania zawartych w nich zasad i procedur.

II. BEZPIECZNE UŻYTKOWANIE SPRZĘTU IT, PROGRAMÓW I DYSKÓW

A osoba, która przetwarza dane osobowe i korzystająca ze sprzętu IT (komputer stacjonarny, monitor, drukarka, skaner, ksero, laptop, tablet, smartfon) ma obowiązek zabezpieczenia go przed zniszczeniem lub uszkodzeniem;

B zgubienie, utrata lub zniszczenie powierzone sprzętu IT powinno być zgłoszone;

C zabrania się samowolnego instalowania sprzętu IT i dodatkowych urządzeń (twarde dyski, pamięć);

D zakazuje się podłączania niezatwierdzonych urządzeń do systemu informatycznego;

E należy uniemożliwić osobom niepowołanym[1] wgląd do danych zawartych na monitorach (*polityka czystego ekranu*);

F czasowe opuszczenie miejsca pracy winno się wiązać z przywołaniem blokowanego hasłem wygaszacza ekranu (*WINDOWS+L*). Dozwolone jest całkowite wylogowanie się z systemu lub programu;

G po zakończeniu pracy należy wylogować się z systemu informatycznego, wyłączyć sprzęt komputerowy, zabezpieczyć stanowisko pracy (szczególnie nośniki, na których znajdują się dane osobowe);

H w trakcie wspólnego użytkowania komputera, użytkownicy zobowiązani są do usuwania plików, do których dostęp mają inni użytkownicy (nieuprawnieni do dostępu do takich plików);

I osoby uprawnione do niszczenia nośników mają obowiązek trwale zniszczyć nośnik lub trwale usunąć z niego dane (niszczenie płyt w niszczarce, niszczenie twardego dysku lub pendrive`a przy pomocy

[1] klient, inny pracownik, pracownik innego działu

młotka).

III. ADMINISTROWANIE UPRAWNIENIAMI- ROZPOCZĘCIE, ZAWIESZENIE I ZAKOŃCZENIE PRACY

A każdy użytkownik[2] musi posiadać swój indywidualny identyfikator (*login*). Zabrania się umożliwiania innym osobom pracy na innym koncie niż swoje własne;

B przełożony wydaje polecenie do utworzenia konta wraz z uprawnieniami. Wykonywane jest to przez informatyków;

C użytkownik nie ma prawa do zmiany swoich uprawnień;

D użytkownik rozpoczyna pracę z użyciem identyfikatora (loginu) i hasła;

E jeśli system zasygnalizuje próby logowania się do systemu osoby nieupoważnionej, należy to niezwłocznie zgłosić informatykowi (administratorowi);

F w chwili zablokowania systemu podczas próby logowania, należy natychmiast powiadomić o tym informatyka (administratora systemu);

G należy uniemożliwić osobom niepowołanym wgląd do danych zawartych na monitorach (*polityka czystego ekranu*);

H czasowe opuszczenie miejsca pracy winno się wiązać z przywołaniem blokowanego hasłem wygaszacza ekranu (*WINDOWS+L*). Dozwolone jest całkowite wylogowanie się z systemu lub programu. Brak tych działań, spowoduje że po upływie **XX** minut system automatycznie aktywuje wygaszacz;

I nie można uruchamiać aplikacji, które nie zostały zweryfikowane przez informatyka (szczególnie dotyczy to programów przesyłanych pocztą elektroniczną);

J po zakończeniu pracy użytkownik musi wylogować się z sytemu informatycznego i wyłączyć sprzęt komputerowy oraz zabezpieczyć stanowisko pracy (w szczególności dokumentację i nośniki, na których znajdują dane osobowe).

IV. POLITYKA HASEŁ

A hasło musi zawierać określoną liczbę znaków, duże i małe litery oraz cyfrę (mogą też zawierać znaki specjalne). Hasło powinno być trudne do odgadnięcia. Nie może być powszechnie używanym słowem. Hasłem nie powinny być: imiona, daty urodzenia, nazwiska oraz

[2] komputera stacjonarnego, laptopa, dysku sieciowego, programów, na których pracownik pracuje, poczty elektronicznej

typowe zestawy (1234..., qwerty);

B nie należy ujawniać haseł innym osobom, ani zapisywać ich na kartkach (w notesie, przy komputerze, na monitorze, pod klawiaturą); jeśli zaistnieje sytuacja ujawnienia hasła osobie trzeciej, należy je natychmiast zmienić;

C hasła muszą być zmieniane co **30/60/90** dni; jeśli nie jest to wymuszone przez system, należy samodzielnie o tym pamiętać; zmiany hasła można dokonać w trakcie pracy w aplikacji;

D pracownicy obowiązani są do zachowania hasła w tajemnicy, nawet po utracie przez nie ważności;

E nie można używać takich samych haseł w serwisach internetowych, jak w systemie komputerowym w jednostce;

F jedno hasło nie może być używane jako zabezpieczenie do różnych systemów;

G zabronione jest generowanie haseł, w których jeden z członów zawsze pozostaje niezmienny, a drugi zmieniany jest według określonego wzorca (np. styczeń 2018, luty2018, marzec2018 itd.).

V. JAK ZABEZPIECZYĆ DOKUMENTACJĘ PAPIEROWĄ Z DANYMI OSOBOWYMI

A każdy pracownik powinien stosować się do *polityki czystego biurka (zał. nr 1)* oraz do *polityki kluczy (zał. nr 2).* Należy zabezpieczać, a w szczególności zamykać, dokumenty i nośniki (szafy, biurka, pomieszczenia zamknięte) przed kradzieżą, lub przed dostęp osób nieupoważnionych po godzinach pracy (lub podczas nieobecności w trakcie pracy);

B pracownicy, którzy przetwarzają dane osobowe są w obowiązku niszczyć dokumenty i wydruki w niszczarkach (ewentualnie utylizować je w specjalnych pojemnikach, które podlegają bezpiecznej utylizacji);

C nie należy pozostawiać dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami[3];

D zakazuje się wyrzucanie niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz.

VI. WYNOSZENIE NOŚNIKÓW Z DANYMI POZA JEDNOSTKĘ

A pracownicy jednostki nie mogą wynosić na zewnątrz jednostki wymiennych nośników[4] informacji z zapisanymi danymi osobowymi

[3] korytarz, toaleta, kserokopiarka, skaner, sala konferencyjna, pomieszczenie socjalne

bez zgody pracodawcy;

B dane osobowe, które zostają wyniesione poza jednostkę należy zaszyfrować; należy uzyskać na to zgodę ADO[5];

C przewożenie dokumentacji papierowej w teczkach musi odbywać się w bezpieczny sposób (np. korzystanie z zaufanych firm kurierskich);

D jeśli przewiezienie dokumentów zawierających dane osobowe zostało powierzone pracownikowi jednostki, musi on w należyty i staranny sposób zabezpieczyć dokumenty przed kradzieżą lub zagubieniem;

E jeśli chcemy przekazać nośniki zawierające dane osobowe poza obszar jednostki należy zastosować odpowiednie środki bezpieczeństwa: powiadomić adresata o przesyłce, zaszyfrować dane, a hasło do ich odczytania przekazać inną drogą, zastosować koperty depozytowe oraz nadać przesyłkę przez kuriera.

VII. BEZPIECZNE KORZYSTANIE Z POCZTY ELEKTRONICZNEJ ORAZ OCHRONA ANTYWIRUSOWA

A dane osobowe przesyłane mailem poza jednostkę odbywa się tylko przez upoważnione do tego osoby. Pliki należy wysłać zaszyfrowane i spakowane[6] oraz zahasłowane. Hasło należy przekazać odbiorcy inną drogą (telefonicznie lub smsem). Hasło powinno się z określonej liczny znaków, powinno zawierać małe i duże litery, cyfry lub znaki specjalne;

B należy dołożyć wszelkiej staranności przy wysyłce dokumentów z danymi osobowymi, poprzez kilkukrotne sprawdzenie poprawności adresu odbiorcy;

C doradza się, aby użytkownik, który przesyła dane osobowe zawarł informację z prośba o potwierdzenie otrzymania wiadomości od odbiorcy;

D ZABRANIA SIĘ: otwierania załączników w mailach, które są wirusami infekującymi komputery w sieci (wiąże się to z bardzo wysokim ryzykiem utraty danych osobowych), klikania w hiperlinki w mailach (są to wirusy atakujące komputery w sieci, co wiąże się to z bardzo wysokim ryzykiem utraty danych osobowych);

E każdorazowo należy zgłaszać informatykowi podejrzane maile (!);

F nie należy wysyłać niezawodowych mail (np. życzeń świątecznych do wszystkich pracowników jednostki);

G wymaga sie kasowania niepotrzebnych maili na bieżąco;

---

[4] wymienne dyski twarde, pendrive`y, płyty CD i DVD
[5] ADO- Administrator Danych Osobowych
[6] PROGRAM ZIP, WINZIP, WINRAR

H	wysyłając maile do wielu adresatów powinno się stosować metodę UDW[7];
I	nie można łączyć firmowych kont pocztowych z prywatnymi;
J	mail służbowy służy tylko do wykonywania obowiązków służbowych; obowiązuje zakaz wysyłania maili z poczty służbowej na prywatne adresy pocztowe pracowników lub innych osób;
K	korzystanie z poczty mailowej do celów prywatnych powinno odbywać się okazjonalnie, i należy to ograniczyć do niezbędnego minimum; nie może to mieć wpływu na jakość pracy i wykonywanie przez niego obowiązków służbowych;
L	nie wolno konfigurować kont pocztowych do automatycznego przekierowania wiadomości na adres zewnętrzny;
M	służbowej poczty mailowej nie można używać w celu rozpowszechniania treści o charakterze obraźliwym lub niemoralnym;
N	użytkownik nie ma prawa bez zgody pracodawcy wysyłać za pośrednictwem poczty mailowej wiadomości, które zawierają dane osobowe dotyczące: pracodawcy, jego pracowników, klientów, kontrahentów , etc.
O	każdy użytkownik zobowiązany jest do skanowania programem antywirusowym plików, które wprowadza z dysków zewnętrznych. Obowiązuje zakaz wyłączania systemu antywirusowego, podczas gdy przetwarzamy dane osobowe w systemie informatycznym. Podczas stwierdzenia zainfekowania systemu należy natychmiast poinformować o tym fakcie informatyka.

VIII. BEZPIECZNE KORZYSTANIE Z INTERNETU

A	Internetu należy używać tylko w sprawach służbowych;
B	każdy, kto korzysta z Internetu ponosi odpowiedzialność za szkody, które powoduje oprogramowanie instalowane z Internetu;
C	surowo wzbronione jest zgrywanie na dysk twardy komputera i korzystanie z nielegalnych programów. Ściąganie plików wymaga zgody osoba zajmującej się infrastrukturą IT w jednostce;
D	zabrania się korzystanie ze stron, które mają charakter hackerski, lub zawierają treści niedozwolone (np. pornograficzne). Strony te najczęściej są zainfekowane i mają automatycznie zainstalowane szkodliwe oprogramowanie, które może zniszczyć zasoby znajdujące się w komputerze użytkownika;
E	nie należy używać w przeglądarce opcji autouzupełniania formularzy zapamiętywania haseł;
F	gdy używamy szyfrowane połączenia w przeglądarce każdorazowo należy sprawdzić, czy pojawia się ikona "kłódki", a adres rozpoczyna się od "https";

[7] UDW- ukryte do wiadomości

G szczególną uwagę należy zwrócić, gdy pojawia się podejrzane żądanie lub prośba logowania na stronę (bank, portal społecznościowy, e-sklep, poczta mailowa). Podejrzane powinno wydać się również, gdy strona wymaga podania loginu, hasła, PIN-u, numeru karty płatniczej przez Internet. Podawanie takich informacji jest zabronione zwłaszcza, gdy dokonujemy płatności przez stronę internetową banku.

IX. JAK POSTĘPOWAĆ, GDY NARUSZONA ZOSTANIE OCHRONA DANYCH OSOBOWYCH

A niezwłocznie i natychmiastowo należy powiadomić o zdarzeniu pracodawcę (nawet w przypadku, gdy istnieje tylko podejrzenie naruszenia ochrony danych osobowych). W szczególności, gdy zauważono nieprawidłowe: zabezpieczenie pomieszczeń, dokumentów i urządzeń, sprzętu IT i oprogramowania; lub gdy nie została zachowana zasada prawidłowej ochrony danych osobowych[8];

B incydenty i zdarzenia, o których należy również powiadamiać to: zewnętrzne zdarzenia losowe (pożary, kradzieże, zalania, utrata łączności), wewnętrzne zdarzenia losowe (awarie sprzętu IT, pomyłki informatyków lub samych użytkowników, zgubienie danych) i umyślnie spowodowane incydenty (kradzież lub wyciek danych osobowych, ujawnienie informacji osobom nieupoważnionym, świadome niszczenie danych lub dokumentów oraz działanie wirusów i szkodliwego oprogramowania);

C w szczególności należy reagować, gdy:

- zauważymy ślady na drzwiach wskazujące na próbę włamania i kradzieży,
- niszczona jest dokumentacja zawierająca dane osobowe bez użycia niszczarki,
- w jednostce znajdują się osoby zachowujące się w podejrzany sposób,
- otwarte pozostają drzwi do szaf i pomieszczeń z danymi osobowymi,
- ustawienia monitorów wskazują na możliwość wglądu osób nieupoważnionych,
- dane osobowe są wynoszone na zewnątrz jednostki (w wersji papierowej i elektronicznej),
- udostępniane są dane osobowe osobom nieupoważnionych,
- odbywają się próby wyłudzenia danych osobowych przez telefon,
- dochodzi do kradzieży lub zagubienia komputerów i innego typu sprzętu, który zawiera dane osobowe,

[8] niestosowanie zasady czystego ekranu/biurka, nienależyta ochrona haseł, niezamykanie szaf i biurek, w których dostępne są dokumenty zawierające dane osobowe.

- otrzymujemy maila z próbą wyłudzenia hasła i loginu,
- zauważymy działania wirusa w komputerze,
- zaobserwujemy zapisane hasła w pobliżu komputera.

X. POUFNOŚĆ I OCHRONA DANYCH OSOBOWYCH

A osoba przetwarzająca dane osobowe jest zobowiązana do przetwarzania danych osobowych tylko w zakresie i celu, który został przewidziany w drodze powierzenia jej przez pracodawcę zadań. Użytkownik przetwarzający dane musi zachować tajemnicę danych osobowych do których ma wgląd i dostęp, w związku z obowiązkami, jakie nałożył na niego pracodawca. Dane osobowe nie mogą być wykorzystywane w celach niezgodnych z zakresem powierzonych zadań przez pracodawcę. W tajemnicy należy zachować sposób zabezpieczenia danych osobowych oraz chronić dane przed zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem i dostępem i przetwarzaniem przez osoby do tego nieupoważnione;

B należy przeszkolić pracowników z zasad ochrony danych osobowym. Pracownicy, którzy przeszły szkolenie i zapoznali się z **Regulaminem ochrony danych osobowych w jednostce** zobowiązane są podpisać **oświadczenie o poufności;**

C kategorycznie zabrania się przekazywania bezpośrednio lub drogą telefoniczną danych osobowych osobom nieupoważnionym, lub osobom, których tożsamość pozostaje trudna do zweryfikowania, lub gdy osoby nieupoważnione podszywają się pod kogoś innego. Instytucjom i osobom, które nie mogą wykazać jasnej podstawy prawnej do dostępu do danych osobowych, również nie należy przekazywać i ujawniać danych osobowych;

D zakaz przekazywania i ujawniania danych osobowych obowiązuje także w grupach dyskusyjnych, forach internetowych i blogach.

XI. CZYNNOŚCI DYSCYPLINARNE

W sytuacji, gdy nastąpi nieuzasadnione zaniedbanie obowiązków wynikających z **regulaminu ochrony danych osobowych w jednostce**, będzie to traktowane jako ciężkie naruszenie obowiązków pracowniczych i zasad współpracy. Sprzeczne działania z zobowiązaniami zawartymi w tym dokumencie może zostać uznane przez pracodawcę jako naruszenie przepisów karnych zawartych w Rozporządzeniu o ochronie danych UE z dnia 27.04.2016 r.

Załącznik nr 3 do Zarządzenia nr 032/2018
Burmistrza Nowego Warpna
z dnia 24 maja 2018 roku

……..…….. ……..……..

Imię i Nazwisko Miejscowość, data

OŚWIADCZENIE

Stwierdzam własnoręcznym podpisem, że zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz znana mi jest treść dokumentacji ochrony danych osobowych przyjętej zarządzeniem nr 032/2018 Burmistrza Nowego Warpna z dnia 24 maja 2018 roku w sprawie wdrożenia Polityk Ochrony Danych Osobowych w Urzędzie Gminy w Nowym Warpnie, wobec czego zobowiązuję się do:

1. stosowania określonych przez Administratora Danych Osobowych zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne w stosunku do celu przetwarzanie danych,
2. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach,
3. należytego zabezpieczenia danych osobowych przed ich udostępnieniem osobom nie upoważnionym,
4. zachowania szczególnej staranności w trakcie dokonywania operacji przetwarzania danych w celu ochrony osób, których dane dotyczą,
5. zachowania w tajemnicy danych do których mam lub będę miał/a dostęp w trakcie wykonywania czynności zleconych przez Pracodawcę oraz ich sposobu zabezpieczeń, nawet po ustaniu stosunku pracy,
6. zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych bezpośredniemu przełożonemu.

W zakresie systemu informatycznego zobowiązuję się:

1. nie ujawniać danych zawartych w eksploatowanych systemach informatycznych, zwłaszcza danych osobowych znajdujących się w tych systemach,
2. nie ujawniać szczegółów technologicznych w używanych systemach oraz oprogramowaniu,
3. nie udostępniać osobom nieupoważnionym nośników magnetycznych i optycznych oraz wydruków komputerowych,
4. nie kopiować lub nie przetwarzać danych w sposób inny niż dopuszczony obowiązującą Dokumentacją.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora Danych Osobowych za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

……..

(podpis)

Załącznik nr 4 do Zarządzenia nr 032/2018
Burmistrza Nowego Warpna
z dnia 24 maja 2018 roku

……..
…… …….....

(imię i nazwisko) *(miejscowość, data)*

OŚWIADCZENIE

Stwierdzam własnoręcznym podpisem, że zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r. oraz znana mi jest treść dokumentacji ochrony danych osobowych przyjętej zarządzeniem nr 032/2018 Burmistrza Nowego Warpna z dnia 24 maja 2018 roku w sprawie wdrożenia Polityk Ochrony Danych Osobowych w Urzędzie Gminy w Nowym Warpnie, wobec czego zobowiązuję się do:

- stosowania określonych przez Administratora Danych Osobowych zasad, procedur oraz wytycznych mających na celu właściwe i adekwatne w stosunku do celu przetwarzanie danych,
- zachowania w tajemnicy danych do których mam lub będę miał/a dostęp w trakcie wykonywania czynności zleconych przez Pracodawcę, oraz ich sposobu zabezpieczeń, nawet po ustaniu stosunku pracy,
- należytego zabezpieczenia danych osobowych przed ich udostępnieniem osobom nie upoważnionym,
- zgłaszania sytuacji (incydentów) naruszenia zasad ochrony danych osobowych Inspektorowi Ochrony Danych lub bezpośredniemu przełożonemu.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora Danych Osobowych za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

……..

(podpis)