BURMISTRZ
MIASTA I GMINY
OSTRORÓG
ul. Wroniecka 14, 64-560 Ostroróg

Zarządzenie Nr 29/2018

Burmistrza Miasta i Gminy Ostroróg

z dnia 22 maja 2018r.

w sprawie wprowadzenia polityki ochrony danych osobowych
w Urzędzie Miasta i Gminy Ostroróg.

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1) zarządzam, co następuje:

§1. W celu zapewnienia bezpieczeństwa danych osobowych gromadzonych i przetwarzanych w Urzędzie Miasta i Gminy Ostroróg zatwierdzam politykę ochrony danych osobowych stanowiącą załącznik nr 1 do zarządzenia.

§2. Traci moc zarządzenie Nr 70/2017 z dnia 6 października 2017 r.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta i Gminy Ostroróg

BURMISTRZ
dr Sławomir Szałata

RADCA PRAWNY
dr Krzysztof Przedowicz

POLITYKA OCHRONY DANYCH OSOBOWYCH

w **Urzędzie Miasta i Gminy Ostroróg**

czerwiec 2018 r.

Zatwierdzona do stosowania przez Burmistrza Miasta i Gminy Ostroróg

Zarządzeniem nr 29/2018 z dnia 22 maja 2018 r.

Spis treści

Spis załączników

Rozdział I
Postanowienia ogólne

§ 1

Polityka Ochrony Danych Osobowych określa zasady w zakresie zarządzania procesami przetwarzania danych osobowych oraz ich bezpieczeństwem w Urzędzie Miasta i Gminy Ostroróg.

§ 2

Niniejszy dokument wykonany został na podstawie zapisów art. 24 ust. 2 i art. 32 ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016r. Parlamentu Europejskiego i Rady (UE) 2016/679 z uwzględnieniem opinii zawartej w motywie 78 tego rozporządzenia.

Rozdział II
Słownik pojęć

§ 3

Występujące w Polityce Ochrony Danych Osobowych zwroty oznaczają:

Administrator – Burmistrz Miasta i Gminy Ostroróg, ;

IOD – Inspektor Ochrony Danych – osoba wyznaczona zarządzeniem przez Burmistrza na podstawie art. 37 ust. 1 RODO, realizujący zadania, o których mowa w art. 39 ust. 1 RODO;

ASI - Administrator Systemów Informatycznych - administrator aplikacji/systemów w UMIG, w których są przetwarzane dane osobowe; osoba odpowiedzialna za realizację zabezpieczeń i odpowiednie funkcjonowanie systemów informatycznych w UMIG, w których przetwarzane są dane osobowe;

dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

identyfikator użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym, zwany dalej także identyfikatorem;

incydent bezpieczeństwa – jakiekolwiek naruszenie poufności, integralności, dostępności, autentyczności, niezawodności i bezpieczeństwa systemu informatycznego, powstałe samoistnie w systemie, bądź dokonane przez osoby nieuprawnione lub uprawnione, działające w złej wierze albo omyłkowo;

klauzula informacyjna – zbiór informacji jakie powinny być przekazane osobie, której dane dotyczą w celu realizacji obowiązków informacyjnych Administratora w stosunku do tych osób, określonych w RODO;

UMIG – Urząd Miasta i Gminy Ostroróg;

komórka organizacyjna – zgodnie z Regulaminem Organizacyjnym UMIG referaty lub jednoosobowe stanowiska pracy;

KKO – kierownik komórki organizacyjnej UMIG – kierownik referatu lub osoba zatrudniona na jednoosobowym stanowisku pracy, zgodnie ze strukturą organizacyjną UMIG określoną w Regulaminie Organizacyjnym, lub osoba aktualnie zastępująca kierownika referatu lub osobę zatrudnioną na jednoosobowym stanowisku pracy;

naruszenie ochrony danych osobowych - 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;

obszar przetwarzania danych osobowych – pomieszczenia, części pomieszczeń lub teren wokół obiektów UMIG, w których przetwarza się dane osobowe w formie papierowej, jak i w systemie informatycznym,

odbiorca danych – osoba fizyczna lub prawna, organ publiczny, jednostka 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;

Organ Nadzorczy – Prezes Urzędu Ochrony Danych Osobowych, niezależny organ publiczny ustanowiony przez Rzeczpospolitą Polską zgodnie z art. 51 RODO;

podmiot przetwarzający - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

PODO - Polityka Ochrony Danych Osobowych w UMIG, zwana dalej także polityką;

przetwarzanie – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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;

system informatyczny przetwarzający dane osobowe – zespół współpracujących ze sobą urządzeń, programów, narzędzi programowych, wraz z procedurami do ich obsługi, zastosowany w celu przetwarzania danych, w celu przetwarzania danych osobowych w UMIG, zwany dalej także systemem;

szczególne kategorie danych osobowych - dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby;

RODO – ogólne rozporządzenie o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679

uodo - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz. U. z 2018r. poz. 1000 ze zm.),

usuwanie danych osobowych – niszczenie danych osobowych lub taką ich modyfikację, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą;

użytkownik – osoba upoważniona do bezpośredniego dostępu do danych osobowych, przetwarzanych w systemie informatycznym lub aplikacji, która posiada ustalony indywidualny identyfikator oraz hasło;

zasób danych osobowych – wszystkie dane osobowe, niezależnie od sposobu ich utrwalenia, występujące w zbiorach, jak i w formie nieuporządkowanej, przetwarzane przez UMIG w celu realizacji jej zadań; w zasobach UMIG wyróżnia się zasoby poszczególnych komórek organizacyjnych;

zbiór danych osobowych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

Rozdział III
Zakres stosowania Polityki i zakres przetwarzania

§ 4

1. Polityka ma zastosowanie do:
    1) danych osobowych przetwarzanych w UMIG niezależnie od sposobu ich utrwalenia,
    2) danych osobowych przetwarzanych, zarówno w zbiorach jak i w formie nieuporządkowanej w zestawach, jak i pojedynczych informacji osobowych,
    3) informacji, dotyczących bezpieczeństwa danych osobowych, w szczególności identyfikatorów i haseł we wszystkich systemach/aplikacjach,
    4) informacji zawartych w rejestrach, instrukcjach i procedurach związanych z przetwarzaniem lub ochroną danych osobowych.
2. W UMIG prowadzone są następujące rejestry czynności przetwarzania danych osobowych, na które to przetwarzanie zgodę wyraził Administrator:
    1) Rejestr Czynności Przetwarzania Danych Osobowych Administratora - dla zbiorów danych osobowych, dla których administratorem jest Burmistrz; wzór rejestru określony został w załączniku nr 1 do PODO,
    2) Rejestr Czynności Przetwarzania Danych Osobowych Podmiotu Przetwarzającego - dla zbiorów danych osobowych, dla których podmiotem przetwarzającym jest Burmistrz; wzór rejestru określony został w załączniku nr 2 do PODO.
3. W UMIG nie powinny być przetwarzane żadne zasoby danych osobowych, w szczególności zbiory danych osobowych, na które to przetwarzanie nie wyraził zgody Administrator.

Rozdział IV
Zarządzanie przetwarzaniem danych osobowych oraz ich bezpieczeństwem

§ 5

1. Administratorem danych osobowych, w rozumieniu art. 4 pkt. 1) RODO, w UMIG jest Burmistrz Miasta i Gminy Ostroróg.
2. Burmistrz Miasta i Gminy Ostroróg jest odpowiedzialny za przetwarzanie i ochronę danych osobowych w UMIG.

3. Strukturę zarządzania przetwarzaniem danych osobowych oraz ich bezpieczeństwem przedstawia graficznie załącznik nr 6 do PODO.
4. W sytuacjach szczególnych Burmistrz może w formie odrębnego aktu wewnętrznego takiego jak zarządzenie doprecyzować postanowienia PODO; doprecyzowanie to powinno być poprzedzone konsultacjami z IOD, a w sytuacji dotyczącej bezpośrednio systemu informatycznego także z ASI.

§ 6

1. Burmistrz wyznacza IOD o czym powiadamia właściwy Organ Nadzorczy.
2. Administrator zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych związane z realizacją jego zadań wynikających z RODO.
3. IOD wykonuje zadania w zakresie:
   1) informowania administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO, innych właściwych przepisów o ochronie danych osobowych, PODO i doradza im w tej sprawie; zadania te IOD realizuje w sposób uwzględniający „Zasady organizacji edukacji z zakresu ochrony danych osobowych" stanowiące załącznik nr 3 do PODO,
   2) monitorowania przestrzegania RODO, innych właściwych przepisów o ochronie danych osobowych oraz PODO, w tym podziału obowiązków, działań zwiększających świadomość, szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów; zadania te IOD realizuje w sposób uwzględniający zasady zawarte w Rozdziale XIV PODO „Monitorowanie przestrzegania RODO, innych właściwych przepisów o ochronie danych osobowych oraz PODO",
   3) udzielania na żądanie zaleceń co do analizy ryzyka naruszenia praw i wolności osób fizycznych, a także oceny skutków dla ochrony danych oraz monitorowania jej wykonania zgodnie z art. 35 RODO,
   4) współpracy z właściwym Organem Nadzorczym,
   5) pełnienia funkcji punktu kontaktowego dla Organu Nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
   6) pełnienie funkcji punktu kontaktowego dla osób, których dane są przetwarzane na zasadach określonych w art. 38 ust. 4 RODO.

§ 7

1. KKO są odpowiedzialni za zarządzanie procesami przetwarzania i ochrony danych osobowych w podległych komórkach organizacyjnych.
2. Do obowiązków KKO, w zakresie zarządzania procesami przetwarzania i ochrony danych osobowych, należy w szczególności:
   1) zarządzanie zasobem danych osobowych w ramach zadań, realizowanych przez podległą komórkę organizacyjną,
   2) nadzór nad ochroną danych osobowych w podległej komórce organizacyjnej,
   3) dopilnowanie, aby terminowo i zgodnie z właściwością, włączać IOD we wszystkie kwestie dotyczące ochrony danych osobowych związane z realizacją jego obowiązków,
   4) dopuszczanie do przetwarzania danych osobowych w podległej komórce organizacyjnej tylko osób posiadających stosowne upoważnienie do przetwarzania danych osobowych wydane przez Administratora i przedłożyły oświadczenie o poufności; informacje w tym zakresie uzyskuje z Referatu Organizacji i Spraw Pracowniczych UMIG,
   5) występowanie z wnioskiem do ASI o nadanie, zmianę lub cofnięcie uprawnień do określonego zasobu danych osobowych przetwarzanych w systemie informatycznym, zgodnie z zakresem upoważnienia do przetwarzania danych osobowych, w sposób określony w „Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych", stanowiącej załącznik nr 5 do PODO,
   6) realizacja zadań szkoleniowych i informacyjnych na zasadach określonych w „Zasadach organizacji edukacji z zakresu ochrony danych osobowych" stanowiących załącznik nr 3 do PODO,
   7) ustalanie z Administratorem zamiaru przetwarzania nowych kategorii danych osobowych, utworzenia nowego zbioru, zasobów danych osobowych lub dokonania zmian w obrębie już przetwarzanych; zgłaszanie faktu dokonanych ustaleń do IOD celem odnotowania ich w określonych rejestrach,
   8) ustalanie w porozumieniu z ASI zasad tworzenia kopii zapasowych plików z danymi osobowymi, znajdującymi się na stacjach roboczych użytkowników w podległej komórce organizacyjnej,
   9) realizacja procesu udostępniania danych osobowych,
   10) realizacja procesu związanego z zapewnieniem praw osobom, których dane dotyczą,

11) realizacja procesu powierzania czynności, związanych z przetwarzaniem danych osobowych innym podmiotom, w tym przygotowanie umów związanych z powierzeniem przetwarzania danych osobowych podmiotowi przetwarzającemu,

12) przedkładanie Administratorowi projektów umów związanych z powierzeniem danych osobowych w celu ich zatwierdzenia i podpisania,

13) opracowywanie klauzul informacyjnych, oświadczeń zgody na przetwarzanie danych osobowych, które powinny być stosowane przy zbieraniu danych osobowych w podległej mu komórce organizacyjnej oraz odpowiadanie za ich stosowanie,

14) umożliwienie IOD przeprowadzenia czynności monitorujących określonych w RODO,

15) wykonywanie innych zadań zgodnie z zapisami PODO.

§ 8

1. Za zabezpieczenie techniczne danych osobowych przetwarzanych w systemie informatycznym odpowiada ASI.
2. Do zdań ASI należy w szczególności:
   1) zapewnienie wdrożenia wymaganych zabezpieczeń technicznych danych osobowych przetwarzanych w systemach informatycznych,
   2) nadzór nad realizacją postanowień „Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych", stanowiącej załącznik nr 5 do PODO,
   3) przekazanie postanowień „Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych" osobom odpowiedzialnym za wykonywanie zadań w niej opisanych,
   4) nadzór nad właściwym funkcjonowaniem systemu informatycznego, w którym przetwarzane są dane osobowe,
   5) nadzór nad rozwiązywaniem sytuacji kryzysowych, pojawiających się w systemie informatycznym,
   6) kontrola działań podejmowanych przez ASI,
   7) realizacja decyzji Administratora o dopuszczeniu do eksploatacji systemów informatycznych, przetwarzających dane osobowe,
   8) nadzorowanie zgodności wszystkich wdrażanych systemów z RODO, właściwymi przepisami z zakresu ochrony danych osobowych, PODO,

9) przedkładanie do Burmistrza wniosków dotyczących propozycji zakupu oprogramowania lub sprzętu, w celu realizacji lub podniesienia poziomu bezpieczeństwa systemów informatycznych, bezpieczeństwa kopii zapasowych / bezpieczeństwa nośników pamięci/itp.,

10) zgłaszanie do Administratora informacji w zakresie bezpieczeństwa systemów informatycznych, niezbędnych do aktualizacji PODO, a w szczególności „Instrukcji Zarządzania Systemem Informatycznym, Służącym Do Przetwarzania Danych Osobowych",

11) dokumentowanie zdarzeń, powodujących naruszenia bezpieczeństwa danych osobowych oraz baz danych systemów informatycznych,

12) przekazywanie IOD informacji o nowych programach i systemach informatycznych, serwerach i innych zmianach systemu informatycznego, ważnych ze względu na realizacje jego obowiązków, w szczególności prowadzenia rejestrów czynności,

13) zapewnienie, wspólnie z kierownikiem referatu właściwego w sprawach technicznych, niezawodności awaryjnego zasilania serwerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania,

14) udział w czynnościach związanych z monitorowaniem przestrzegania RODO, innych właściwych przepisów o ochronie danych osobowych oraz PODO, prowadzonych na zasadach określonych w Polityce,

15) podjęcie niezbędnych i odpowiednich do zagrożeń działań w zakresie zabezpieczenia systemów informatycznych w sytuacji naruszenia ochrony danych osobowych,

16) wykonywanie innych zadań zgodnie z zapisami PODO,

17) fizyczne nadawanie dostępu do systemu informatycznego osobom upoważnionym do przetwarzania danych osobowych,

18) usuwanie i modyfikacja uprawnień do dostępu do danych osobowych w systemie informatycznym,

19) ustalanie i kontrola identyfikatorów dostępu do systemu informatycznego,

20) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,

21) przeciwdziałanie dostępowi osób nieupoważnionych do systemu informatycznego, w którym przetwarzane są dane osobowe,

22) realizacja zadań, obejmujących procesy przetwarzania i archiwizowania danych oraz wspomaganie użytkowników w sytuacjach problemowych,

23) kontrolowanie bezpieczeństwa wszystkich systemów informatycznych, służących do przetwarzania danych osobowych w UMIG,

24) nadzór nad realizacją napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe,

25) wykonywanie kopii zapasowych aplikacji i danych systemów informatycznych w stosunku do danych gromadzonych na serwerach UMiG, zabezpieczenie ich przechowywania oraz okresowe ich sprawdzanie pod kątem dalszej przydatności do odtwarzania danych w przypadku awarii systemu,

26) zapewnienie bezpieczniej wymiany danych w sieci wewnętrznej i nadzór nad przesyłaniem danych za pośrednictwem urządzeń teletransmisji,

27) wykonywanie innych czynności zgodnie z zapisami PODO, a także poleceń Administratora lub ASI w zakresie ochrony, działań monitorujących i przetwarzania, dotyczących danych osobowych.

§ 9

Rozdział V
Polecanie osobom przetwarzania danych osobowych

§ 10

1. Burmistrz jest upoważniony do przetwarzania wszelkich danych osobowych, występujących w zasobach UMIG.
2. Burmistrz upoważnia osoby zatrudnione w UMIG bez względu na charakter zatrudnienia, odbywające staż lub praktykę, realizujące zadania na podstawie umowy cywilnoprawnej, realizujące zadania w ramach prac w komisjach, zespołach, grupach roboczych realizujące zadania w ramach służby dyżurnej podczas szkoleń lub w stanowisku kierowania, do przetwarzania danych osobowych w zakresie niezbędnym do realizacji zadań podczas wykonywanej pracy lub innych czynności.
3. Osoby, które nie zostały upoważnione do przetwarzania danych osobowych na zasadach określonych w PODO nie powinny przetwarzać danych osobowych.
4. Upoważnianie wskazanych osób do przetwarzania danych osobowych powinno być poprzedzone szkoleniem przeprowadzonym według zasad określonych w „Zasadach organizacji edukacji z zakresu ochrony danych osobowych" stanowiących załącznik nr 3 do PODO.
5. Upoważnienie do przetwarzania danych osobowych dla osób zatrudnionych w UMIG bez względu na charakter zatrudnienia, odbywających staż lub praktykę, realizujących zadania na podstawie umowy cywilnoprawnej, poza sytuacjami szczególnymi

określonymi przez Administratora, powinno mieć charakter pisemny; wzór takiego upoważnienia stanowi załącznik nr 7 do PODO.

6. Burmistrz może pisemnie upoważnić inną osobę do nadawania i podpisywania upoważnień do przetwarzania danych osobowych, o których mowa w § 10 pkt. 5,
7. Upoważnienie do nadawania i podpisywania upoważnień do przetwarzania danych osobowych przygotowuje referat właściwy w sprawach kadrowych; jego wzór stanowi załącznik nr 8 do PODO,
8. Upoważnienie do przetwarzania danych osobowych, o którym mowa w § 10 pkt. 5 przygotowuje referat właściwy w sprawach kadrowych, po otrzymaniu wypełnionej „Informacji o przeprowadzeniu szkolenia przed przystąpieniem do pracy/służby/stażu/praktyk", której wzór określony został w załączniku nr 4 do PODO.
9. Osoby upoważnione do przetwarzania danych osobowych, wraz z nadaniem im upoważnienia do przetwarzania danych osobowych, składają w referacie właściwym w sprawach kadrowych oświadczenie osoby upoważnionej o zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia; wzór oświadczenia stanowi załącznik nr 9 do PODO.
10. „Upoważnienia do przetwarzania danych osobowych", „Upoważnienia do nadawania i podpisywania upoważnień" oraz oświadczenia, o których mowa w § 10 pkt. 10, przechowuje zgodnie z przepisami właściwymi w sprawach kancelaryjnych referat właściwy w sprawach kadrowych.
11. IOD prowadzi rejestr upoważnień zgodnie ze wzorem określonym w załączniku nr 7a.
12. Zasady postępowania przy nadaniu, modyfikacji lub anulowaniu uprawnień do przetwarzania danych osobowych w systemie informatycznym określone zostały w „Instrukcji Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych", stanowiącej załącznik nr 5 do PODO.
13. Upoważnienie do przetwarzania danych osobowych, jak również upoważnienie do nadawania i podpisywania upoważnień wygasa automatycznie wraz z ustaniem stosunku zatrudnienia, zakończeniem wykonywania prac, określonych umową cywilnoprawną / o staż / praktykę, a także obowiązków związanych z pracą w komisjach, zespołach, grupach roboczych, oraz realizowanych w ramach służby dyżurnej podczas szkoleń lub w stanowisku kierowania.
14. Upoważnienia, o których mowa w § 10 pkt. 2, Administrator może cofnąć o każdym czasie, w szczególności na wniosek IOD, ASI lub KKO.

§ 11

Osoby, które nie przetwarzają danych osobowych ale w związku z realizacją swoich obowiązków znają zasady ich zabezpieczania, realizują swoje obowiązki w celu realizacji czynności związanych z zatrudnieniem lub zawartą umową cywilnoprawną; osoby te powinny złożyć w referacie właściwym w sprawach kadrowych oświadczenie, o którym mowa w § 6 pkt. 10; decyzję w tej sprawie podejmuje właściwy KKO.

§ 12

Strukturę organizacyjną związaną z poleceniem osobom przetwarzania danych osobowych przedstawiono w formie graficznej w załączniku nr 10 do PODO.

Rozdział VI
Polecenie przetwarzania danych osobowych podmiotowi przetwarzającemu

§ 13

1. Zlecanie jakichkolwiek czynności, związanych z przetwarzaniem danych osobowych podmiotom przetwarzającemu, jest formą powierzenia przetwarzania danych osobowych.
2. Decyzję o powierzeniu przetwarzania danych osobowych podejmuje Burmistrz lub osoba przez niego upoważniona do zawierania umów.
3. Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy; wzór zapisów umowy w zakresie ochrony danych osobowych stanowi załącznik nr 11 do PODO.
4. KKO przygotowuje projekt umowy, na podstawie której dochodzi do powierzenia przetwarzania danych osobowych.
5. KKO uzgadnia projekt umowy z właściwym radcą prawnym, a jeżeli powierzenie danych osobowych jest związane z przetwarzaniem danych w systemie informatycznym. takim jak: przesył danych czy zdalne udostępnianie danych, także z ASI w zakresie zapisów dotyczących:
   1) udostępniania danych w systemie informatycznym,
   2) przesyłania danych drogą teletransmisji.

6. KKO przedkłada umowę do podpisu zgodnie z § 13 pkt. 2.

§ 14

W sytuacji gdy przedmiotem innej umowy, zawartej z podmiotem nie będącym podmiotem przetwarzającym, nie jest powierzenie przetwarzania danych osobowych, ale w celu realizacji przedmiotu umowy pracownicy tego podmiotu poznają sposoby ochrony danych osobowych w UMIG, KKO przygotowujący umowę powinien zawrzeć w niej zapisy dotyczące ochrony danych osobowych, a następnie przed rozpoczęciem realizacji czynności przez tych pracowników aby odebrał od nich oświadczenia o poufności.

Rozdział VII
Zasady przetwarzania danych osobowych

§ 15

1. Dane osobowe w utworzonych zbiorach muszą być zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.
2. Zbierane dane osobowe muszą być merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.
3. Zabronione jest zbieranie wszelkich danych nieistotnych, nie mających znaczenia, o większym stopniu szczegółowości niż wynika to z określonego celu.
4. Zabronione jest przetwarzanie danych osobowych, dla których zakres, cel przetwarzania i sposoby przetwarzania nie został ustalony przez Burmistrza, z wyjątkiem danych osobowych wynikających wprost z przepisów prawa.
5. Dane mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
6. Okres przechowywania może zostać wydłużony nawet po osiągnięciu celu przetwarzania, jeżeli przepisy ustaw szczególnych takie postępowanie dopuszczają.

§ 16

1. Dane osobowe w zbiorach danych osobowych mogą być przetwarzane po ich wcześniejszej rejestracji w „Rejestrze Czynności Przetwarzania Danych Osobowych Administratora" lub w „Rejestrze Czynności Przetwarzania Danych Osobowych Podmiotu Przetwarzającego".
2. W celu dokonania rejestracji KKO zgłasza Burmistrzowi zamiar przetwarzania nowych kategorii danych osobowych, utworzenia nowego zbioru, zasobów danych osobowych lub dokonania zmian w obrębie już przetwarzanych.
3. Zgłoszenie powinno zawierać w szczególności:
   1) kategorie osób, których dane dotyczą,
   2) kategorie danych osobowych (zakres danych osobowych),
   3) cel przetwarzania,
   4) kategorie ewentualnych odbiorców, którym dane osobowe byłyby ujawniane,
   5) planowane terminy usunięcia danych osobowych,
   6) opis technicznych i organizacyjnych środków bezpieczeństwa, w szczególności tych, o których mowa art. 32 ust. 1. RODO,
   7) nazwę i dane kontaktowe ewentualnych współadministratorów
   8) jeśli ma to zastosowanie - dane, o których mowa w art. 30 ust. 1 lit. e) RODO.
4. Burmistrz, w przypadku wątpliwości może żądać opinii IOD w tej sprawie.
5. W sytuacji akceptacji Burmistrza na rozpoczęcie przetwarzania zgodnie z zamiarem, o którym mowa w § 16 pkt. 2, KKO jest zobowiązany przedstawić zgłoszenie Z-cy IOD celem dokonania stosownych wpisów w rejestrach czynności Administratora lub Podmiotu Przetwarzającego.

Rozdział VIII

Zgodność przetwarzania z prawem

§ 17

1. W sytuacji gdy podstawą prawną przetwarzania danych osobowych nie będzie żaden z zapisów art. 6 ust. 1 lit. b),c),d),e) RODO przetwarzanie jest możliwe na podstawie zgody na przetwarzanie danych osobowych wyrażonej przez osobę, której dane dotyczą.
2. Zgoda na przetwarzanie danych osobowych powinna być odbierana w formie pisemnego oświadczenia osoby, której dane dotyczą; wzór oświadczenia stanowi załącznik nr 13 do PODO.

3. Zgoda na przetwarzanie danych osobowych, która jest częścią składową kwestionariuszy, formularzy, itp., powinna być odebrana (podpisana) odrębnie.
4. Zapisy §18 pkt. 2,3,4 stosuje się odpowiednio do oświadczeń zgody na przetwarzanie danych osobowych.
5. W sytuacjach szczególnych, określonych przez Administratora, zgoda może być odebrana w formie jednoznacznego, wyraźnego działania.

Rozdział IX

Realizacja obowiązków informacyjnych

§ 18

1. W przypadku zbierania danych osobowych bezpośrednio od osób - na formularzach, kwestionariuszach, drukach i innych służących do zbierania danych osobowych – prowadzonych zarówno w formie papierowej, jak i elektronicznej, należy umieszczać na nich klauzulę informacyjną; wzór klauzuli stanowi załącznik nr 12 do PODO.
2. KKO opracowuje klauzule informacyjne, które powinny być stosowane przy zbieraniu danych osobowych w podległej mu komórce organizacyjnej.
3. W przypadku wątpliwości związanych ze stosowaniem i opracowaniem klauzuli Administrator może zażądać opinii IOD.
4. KKO odpowiada za stosowanie klauzul informacyjnych.

§ 19

1. W przypadku pozyskiwania danych osobowych w inny sposób niż od osoby, której dane osobowe dotyczą, Administrator jest zobowiązany realizować obowiązek informacyjny w stosunku do tych osób w sposób określony w art. 14 RODO.
2. Zapisy §18 pkt. 2,3,4 stosuje się odpowiednio.

Rozdział X

Prawa osoby, której dane osobowe dotyczą

§ 20

1. Zasady i warunki korzystania z praw osoby, której dane osobowe dotyczą określone zostały w Rozdziale III RODO: „Prawa osoby, której dane dotyczą".
2. Wnioski w sprawie skorzystania z praw osoby, której dane osobowe dotyczą rozpatruje i realizuje właściwy KKO; w przypadku wątpliwości co do zgodności z prawem przyjętego postępowania, a w szczególności w sytuacji wątpliwości co odpowiedzi odmownej lub udostępniania danych, KKO na polecenie administratora może zasięgnąć opinii IOD.
3. W celu ułatwienia korzystania z praw przez osobę, której dane dotyczą Administrator umożliwia jej kontakt z IOD poprzez umieszczeniu adresu mailowego do niego na stronie internetowej UMIG.
4. W przypadku skontaktowania się osoby, której dane dotyczą bezpośrednio z IOD, Administrator lub wskazani przez niego KKO są zobowiązani niezwłocznie udzielić mu wszelkiej możliwej pomocy i informacji w celu rozwiązania problemu oraz do spowodowania aby osoba, która się do niego zwróciła mogła skorzystać ze swoich praw.
5. Informacja o osobie, której dane dotyczą powinna być przekazana w ciągu 1 miesiąca z możliwością przedłużenia jej przekazania o kolejne 2 miesiące jeżeli wniosek / żądanie ma skomplikowany charakter.

§ 21

1. Dane osobowe mogą być udostępniane w następujących przypadkach:
   1) na podstawie przepisów prawa organom publicznym w ramach konkretnego postępowania,
   2) na podstawie wniosku od podmiotu uprawnionego do otrzymania danych na podstawie przepisów prawa,
   3) na podstawie umowy z odbiorcą danych lub współadministratorem danych, w ramach której istnieje konieczność udostępnienia danych.
2. Proces udostępniania danych osobowych rozpatruje i realizuje właściwy KKO; w przypadku wątpliwości co do zgodności z prawem przyjętego postępowania, KKO na polecenie Administratora może zasięgnąć opinii IOD.

3. Informacje zawierające dane osobowe, przekazywane są uprawnionym podmiotom lub osobom, za potwierdzeniem odbioru, w następujący sposób:
   1) pocztą kurierską,
   2) listem poleconym za pokwitowaniem odbioru,
   3) za pomocą teletransmisji danych,
   4) osobiście za potwierdzeniem odbioru.
   5) w inny, określony konkretnym wymogiem prawnym lub umową, sposób.
4. ASI nadzoruje przestrzeganie zasad bezpieczeństwa, w przypadku udostępniania danych osobowych drogą elektroniczną.
5. Osoby przetwarzające dane osobowe zachowują szczególną ostrożność przy przekazywaniu danych osobowych drogą telefoniczną; przekazanie tą drogą może nastąpić tylko w sytuacji pełnej pewności co do tożsamości osoby, której dane są przekazywane.

Rozdział XI

Obszar przetwarzania danych osobowych

§ 22

1. Obszarem przetwarzania danych osobowych w UMIG są budynki, pomieszczenia lub części pomieszczeń, w których są przetwarzane dane osobowe zarówno w formie papierowej, jak i w systemie informatycznym, zlokalizowane:
   1) w siedzibie Urzędu Miasta i Gminy w Ostrorogu, ul. Wroniecka 14,
   2) w komórkach organizacyjnych zorganizowanych poza tą siedzibą.
2. Przebywanie wewnątrz obszaru przetwarzania danych osobowych, osób nieuprawnionych do dostępu do danych osobowych - jest dopuszczalne za zgodą Administratora lub w obecności osoby dopuszczonej do przetwarzania tych danych lub za zgodą KKO.
3. Pracownicy firm zewnętrznych, przebywający wewnątrz obszaru przetwarzania danych osobowych poza godzinami pracy lub bez obecności osoby dopuszczonej do przetwarzania danych powinny podpisać oświadczenia, o których mowa w § 14 pkt. 1 PODO i powinny one być dołączone do umów z tymi firmami.
4. Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób dopuszczonych do danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.

§ 23

1. W sytuacji konieczności przetwarzania danych osobowych, poza obszarem wymienionym w § 22 pkt. 1 PODO zgodę na takie działania wydaje Administrator lub KKO.
2. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych.
3. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada osoba dokonująca ich wyniesienia.

Rozdział XII
Przetwarzanie danych osobowych w systemie informatycznym i na nośnikach papierowych

§ 24

Zasady zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, określa dokument „Instrukcja Zarządzania Systemem Informatycznym Służącym Do Przetwarzania Danych Osobowych", stanowiąca załącznik nr 5 do PODO,

§ 25

1. Dane osobowe, zawarte w dokumentacji papierowej, mogą być przetwarzane jedynie przez osoby upoważnione do przetwarzania danych osobowych zgodnie z zasadami określonymi w PODO.
2. Kopie papierowe z danymi osobowymi muszą być przechowywane w zamykanych na klucz szafach, szufladach lub sejfach; obowiązuje tzw. „zasada czystego biurka".
3. Dopuszcza się przechowywanie danych osobowych w niezamykanych szafach lub regałach tylko w pomieszczeniu archiwum zabezpieczonym zgodnie z odrębnymi przepisami.
4. Niszczenie dokumentów papierowych powinno przebiegać z wykorzystaniem specjalnych urządzeń do wykonywania tych czynności takich jak niszczarki.
5. Zasady przechowywania, sposób archiwizowania i likwidacji dokumentów papierowych, określają przepisy kancelaryjne UMIG. W zakresie nieuregulowanym przepisami kancelaryjnymi UMIG, odpowiednie zasady określa KKO po konsultacji z Administratorem; w sytuacjach szczególnych mogą w tej sprawie zasięgnąć porady IOD.

Rozdział XIII
Postępowanie w sytuacji naruszenia ochrony danych osobowych

§ 26

1. W sytuacji naruszenia lub podejrzenia naruszenia zasad ochrony danych osobowych należy postępować zgodnie z regułami opisanymi w „Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych", której wzór stanowi załącznik nr 14 do PODO.

Rozdział XIV
Monitorowanie przestrzegania RODO, innych właściwych przepisów o ochronie danych osobowych oraz PODO

§ 27

1. Działania związane z monitorowaniem przestrzegania przepisów w zakresie ochrony danych osobowych obejmują działania planowe i pozaplanowe; do działań planowych zalicza się w szczególności działania audytowe i kontrolne, ocenę ochrony przetwarzania danych osobowych prowadzoną na podstawie informacji uzyskanych od Administratora w zakresie ustalonym przez IOD; działania pozaplanowe wynikają z zakresu obowiązków IOD.
2. IOD przygotowuje Plan Działań Związanych z Monitorowaniem Przestrzegania Przepisów w Zakresie Ochrony Danych Osobowych.
3. Plan Działań Monitorujących w UMiG Ostroróg powinien zawierać co najmniej jedno działanie audytowe realizowane nie rzadziej niż raz na rok.
4. W trakcie realizacji działań monitorujących, w tym audytów IOD może dokumentować swoje czynności:
   a) notatką z podjętych czynności,
   b) protokołem odebrania ustnych wyjaśnień,
   c) innymi sposobami, w tym informacjami zebranymi na piśmie lub drogą elektroniczną.
5. Z przeprowadzonych czynności monitorujących IOD przekazuje informację wraz z wnioskami Administratorowi; w przypadku działań audytowych IOD sporządza „Sprawozdanie z działań planowych/pozaplanowych związanych z monitorowaniem/naruszeniem przestrzegania przepisów w zakresie ochrony danych osobowych".

Rozdział XV

Ocena ryzyka naruszenia praw lub wolności osób fizycznych

§ 28

1. Zasady oceny ryzyka naruszenia praw lub wolności osób fizycznych określa dokument „Arkusz szacowania ryzyka naruszenia praw lub wolności osób fizycznych" stanowiący załącznik nr 15 do PODO.
2. Ocenę skutków dla ochrony danych osobowych prowadzi się w sytuacjach i na zasadach określonych w art. 35 RODO.

Rozdział XVI
Odpowiedzialność karna

§ 29

1. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi, określonymi w uodo oraz w art. 130, 266 - 269, 287 Kodeksu Karnego.
2. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w § 30 pkt 1, naruszenie zasad ochrony danych osobowych obowiązujących w UmiG Ostroróg, może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Rozdział XVII
Postanowienia końcowe

§ 30

1. Polityka wchodzi w życie z dniem 22 maja 2018 r.

Załącznik Nr 1
do Polityki Ochrony Danych Osobowych
w UMiG w Ostrorogu

WZÓR REJESTRU CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH ADMINISTRATORA

Nazwa Administratora																
Dane kontaktowe																
Imię i nazwisko Inspektora Ochrony Danych																
LP.	Nazwa czynności przetwarzania	Jednostka organizacyjna (Referat, Wydział itp.)	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*	Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*	Nazwa podmiotu przetwarzającego i dane kontaktowe *(jeśli dotyczy)*	Kategorie odbiorców *(innych niż podmiot przetwarzający)*	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 *(jeżeli jest to możliwe)*	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub org. międzynarodowej	
															Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
			Art.. 30 ust. 1 pkt b	Art.. 30 ust. 1 pkt c	Art.. 30 ust. 1 pkt c			Art.. 30 ust. 1 pkt f	Art.30 ust. 1 pkt a	Art.. 30 ust. 1 pkt d	Art.. 30 ust. 1 pkt d		Art.. 30 ust. 1 pkt g		Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 2
do Polityki Ochrony Danych Osobowych
w UMiG w Ostrorogu

WZÓR REJESTRU CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH PODMIOTU PRZETWARZAJĄCEGO

Nazwa Podmiotu Przetwarzającego	
Dane kontaktowe Podmiotu Przetwarzającego	
Imię i nazwisko Inspektora Ochrony Danych	

Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe podwykonawców	Kategorie przetwarzań dokonywanych w imieniu każdego z administratorów	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1. RODO	Dane, o których mowa w art. 30 ust. 2 lit. c) RODO
1.	2.	3.	4.	5.

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 3
do Polityki Ochrony Danych Osobowych
w UMiG w Ostrorogu

Zasady organizacji edukacji z zakresu ochrony danych osobowych

1. Celami działań edukacyjnych są zapoznanie osób przetwarzających dane osobowe w UMiG z regulacjami prawnymi w zakresie ochrony danych osobowych i zasadami bezpiecznego przetwarzania danych osobowych w UMiG.
2. Wyróżnia się następujące rodzaje działań edukacyjnych:
   a) szkolenie przed przystąpieniem do pracy/służby/stażu/praktyk,
   b) instruktaż stanowiskowy w zakresie ochrony danych osobowych,
   c) informowanie o zmianach w zakresie ochrony danych osobowych,
   d) szkolenie fakultatywne.
3. Zasady organizacji szkolenia przed przystąpieniem do pracy/służby/stażu/praktyk:
   a) szkolenie powinno być przeprowadzone dla osób, które będą przetwarzały dane osobowe, przed rozpoczęciem pracy/służby/stażu/praktyk w UMiG polegającej na przetwarzaniu danych osobowych,
   b) celem szkolenia jest zapoznanie tych osób z regulacjami prawnymi w zakresie ochrony danych osobowych, w tym regulacjami wewnątrzzakładowymi z zakresu ochrony danych osobowych obowiązującymi na terenie UMiG,
   c) organizacja i przeprowadzenie szkolenia dla pracowników, stażystów i praktykantów jest obowiązkiem IOD, za wyjątkiem określonym w lit. d), e)
   d) w celu zapewnienia ciągłości działania UMiG, w sytuacji absencji IOD, szkolenie dla pracowników, stażystów i praktykantów przeprowadza KKO
   e) Administrator może także nakazać w innych sytuacjach, do których zalicza się także wprowadzenie nowych regulacji z zakresu ochrony danych osobowych dla całej UMiG, zorganizowane szkolenia w formie samokształcenia kierowanego z wykorzystaniem narzędzi internetowych,
   f) IOD może opracować pomocniczy materiał szkoleniowy dla KKO i IOD, którzy będą przeprowadzali szkolenie,
   g) czas szkolenia powinien zapewniać realizację celu przy uwzględnieniu doświadczenia uczestnika szkolenia w zakresie ochrony danych osobowych,
   h) szkolenie dokumentuje się poprzez wystawienie „Informacji o przeprowadzeniu szkolenia" stanowiącej załącznik nr 4 do PBDO,
   i) przygotowaniem i przechowywaniem „Informacji o przeprowadzeniu szkolenia przed przystąpieniem do pracy/służby/stażu/praktyk" w aktach osobowych wraz z upoważnieniem do przetwarzania danych osobowych, zajmuje się wydział właściwy w sprawach kadrowych.
4. Zasady organizacji instruktażu stanowiskowego w zakresie ochrony danych osobowych:
   a) szkolenie powinno być przeprowadzone dla:
      — osób, które będą przetwarzały dane osobowe, przed dopuszczeniem do wykonywania tej pracy/służby/stażu/praktyk w UMiG,

— osób, które już przetwarzały dane osobowe w UMiG, ale obecnie zmieniają się przy ich pracy warunki jej wykonywania, związane z ochroną danych osobowych,

b) instruktaż może zostać przeprowadzony tylko dla osób wskazanych powyżej pkt. 4 lit. a) tego załącznika i jednocześnie odbyły szkolenie, o którym mowa w pkt. 3.

c) celem szkolenia jest zapoznanie osób, które będą przetwarzały dane osobowe, z zasadami ochrony danych osobowych na danym stanowisku pracy,

d) szkolenie organizuje i przeprowadza KKO,

e) czas szkolenia należy dostosować do warunków ochrony danych osobowych na stanowisku pracy oraz doświadczenia osób w zakresie ochrony danych osobowych.

5. W przypadku osób, które będą przetwarzały dane osobowe w UMiG, a nie będących pracownikami, stażystami lub praktykantami w UMiG, szkolenie o którym mowa w pkt. 3 i 4 tego załącznika przeprowadza właściwy KKO; osobami takimi są w szczególności osoby wyznaczone do prac w komisjach, zespołach i innych grupach roboczych oraz realizujące zadania w ramach służby dyżurnej podczas szkoleń lub w stanowisku kierowania. W tym przypadku nie ma konieczności wystawiania Informacji o przeprowadzeniu szkolenia.

6. Zasady informowania o zmianach w zakresie ochrony danych osobowych:
   a) informowanie o zmianach w zakresie ochrony danych osobowych jest obowiązkiem:
      — IOD w stosunku do Administratora,
      — KKO w stosunku do osób, które przetwarzają dane osobowe w podległej komórce organizacyjnej,
   b) poinformowanie może być prowadzone w formie instruktażu, wykładu, samokształcenia z wykorzystaniem informacji przesłanej drogą elektroniczną lub informacji w formie papierowej, informacji ustnej,
   c) celem przekazania informacji jest jak najszybsze zapoznanie osób, które przetwarzają dane osobowe, z zmienionymi przepisami i zasadami z zakresu ochrony danych osobowych.

7. Zasady organizacji szkoleń fakultatywnych:
   a) organizacja szkoleń fakultatywnych określana jest doraźnie dla każdego szkolenia oddzielnie,
   b) o potrzebie zorganizowania szkolenia decyduje sam Administrator, lub czyni to na wniosek IOD, ASI, KKO lub grupy pracowników.

BURMISTRZ

dr Sławomir Szałata

Załącznik Nr 4
do Polityki Ochrony Danych Osobowych
w UMiG w Ostrorogu

WZÓR INFORMACJI O PRZEPROWADZENIU SZKOLENIA PRZED PRZYSTĄPIENIEM DO PRACY/SŁUŻBY/STAŻU/PRAKTYK

W dniu ..... przeprowadzone zostało „szkolenie przed przystąpieniem do pracy / służby / stażu / praktyk [1)] dla osoby, która będzie w ramach swoich obowiązków w UMiG w Ostrorogu przetwarzała dane osobowe.

W trakcie szkolenia zapoznano Panią(a) ..... z regulacjami prawnymi w zakresie ochrony danych osobowych, w szczególności przekazano informację o obowiązkach spoczywających na osobach przetwarzających dane osobowe na mocy:

- ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679 o ochronie danych osobowych,
- innych przepisów Unii lub przepisów polskich o ochronie danych osobowych,
- regulacji wewnątrzzakładowych, takich jak polityki, instrukcje, procedury z zakresu ochrony danych osobowych obowiązujące na terenie UMiG w Ostrorogu.

Szkolenie przeprowadzono zgodnie z zapisami Polityki Ochrony Danych Osobowych w UMiG w Ostrorogu.

.....	.....
(czytelny podpis osoby szkolonej)	*(czytelny podpis prowadzącego szkolenie)*

OBJAŚNIENIA.

1) właściwe podkreślić lub podać inne,

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 5
do Polityki Ochrony Danych Osobowych
w UMiG w Ostrorogu

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 1
Przedmiot Instrukcji.

Przedmiotem Instrukcji jest określenie zagadnień związanych z bezpieczeństwem danych osobowych przetwarzanych w systemach informatycznych, w szczególności gromadzonych, transmitowanych i przechowywanych w systemach informatycznych, a także sposobu zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

Instrukcja określa w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) rejestrowanie uprawnień do przetwarzania danych osobowych w systemie informatycznym;
3) stosowane metody i środki uwierzytelnienia oraz procedury, związane z ich zarządzaniem i użytkowaniem;
4) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
5) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych, służących do ich przetwarzania;
6) sposób, miejsce i okres przechowywania:
    a) elektronicznych nośników informacji zawierających dane osobowe,
    b) kopii zapasowych, o których mowa w § 1 pkt. 5 powyżej;
7) sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, a także przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
8) udostępnianie danych osobowych;
9) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji, służących do przetwarzania danych;
10) przetwarzanie danych osobowych na laptopach;
11) przetwarzanie danych osobowych na urządzeniach przenośnych, innych niż laptopy.

§ 2

Procedury nadawania, modyfikacji i anulowania uprawnień do przetwarzania danych osobowych w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Dostęp do systemu informatycznego (rozumiany również jako nadanie, odebranie lub zmiana uprawnień) nadawany jest użytkownikowi na wniosek KKO.
2. Uprawnienia w systemie informatycznym przyznawane użytkownikowi, wynikają z zakresu jego obowiązków i powinny być zgodne z upoważnieniem do przetwarzania danych osobowych.
3. Użytkownikom należy przyznawać minimalne uprawnienia, niezbędne do realizacji zadań, wynikających z ich zakresu obowiązków.
4. Wraz z przekazaniem przez KKO do referatu ds. kadrowych UMiG w Ostrorogu „Informacji o przeprowadzeniu szkolenia", której wzór stanowi załącznik nr 4 do PODO, KKO jest zobowiązany wystąpić drogą mailową do ASI o nadanie identyfikatora do systemu dla osoby upoważnianej, z podaniem programów i zasobów, których będzie używał pracownik upoważniony do przetwarzania danych osobowych.
5. ASI nadany identyfikator przekazuje drogą mailową do referatu ds. kadrowych UMiG w Ostrorogu w celu umożliwienia przygotowania przez ten referat upoważnienia do przetwarzania danych osobowych, którego wzór stanowi załącznik nr 7 do PODO.
6. ASI wprowadza nadany identyfikator do systemu dopiero po otrzymaniu potwierdzenia o podpisaniu upoważnienia do przetwarzania danych osobowych od referatu ds. kadrowych UMiG .
7. Informacja o ustaniu stosunku zatrudnienia lub zakończeniu przez użytkownika wykonywania prac, określonych umową zlecenia / umową o dzieło / o staż / praktykę powinna być przekazana niezwłocznie przez kierownika referatu ds. kadrowych UMiG do ASI. W takim przypadku ASI natychmiast po otrzymaniu informacji z referatu ds. kadrowych UMiG w Ostrorogu blokuje dostęp użytkownikowi do systemu.
8. Zmiana nadanych wprowadzeniem identyfikatora do systemu uprawnień jest możliwa na wniosek KKO przesłany drogą mailową do ASI.
9. ASI przy realizacji zadań z zakresu dostępu do systemu informatycznego, a w szczególności przy zakładaniu konta o odpowiednim identyfikatorze, zabezpiecza go hasłem lub kartą mikroprocesorową.
10. Konto użytkownika zostaje zablokowane przez ASI na polecenie ADO lub na wniosek KKO oraz na polecenie ASI w przypadku wystąpienia incydentu bezpieczeństwa.
11. W przypadku naruszania przez użytkownika zasad pracy w systemie informatycznym, ASI może zablokować konto do czasu wyjaśnienia nieprawidłowości. ASI o fakcie zablokowania konta informuje Administratora.
12. ASI lub wyznaczony przez niego ASI dokonuje okresowych przeglądów kont użytkowników w celu wykrycia kont nieaktywnych.
13. Powyższe zasady obowiązują również osoby uzyskujące dostęp do danych osobowych na podstawie umowy zlecenia.

14. Prace związane z przetwarzaniem danych osobowych w systemie informatycznym, w związku z pracą w zespołach, komisjach, lub podczas pełnienia służby podczas procesu szkoleniowego powinna wykonywać osoba będąca pracownikiem UMiG w Ostrorogu , która posiada już nadany identyfikator do pracy w systemie,

§ 3
Rejestrowanie uprawnień do przetwarzania danych osobowych w systemie informatycznym.

1. Przyznanie uprawnień w zakresie dostępu do danych przetwarzanych w systemach informatycznych polega na przypisaniu przez ASI w systemie dla upoważnionego użytkownika:
   a. unikalnego identyfikatora i hasła lub unikalnego identyfikatora i przypisanej do niego karty mikroprocesorowej;
   b. wprowadzeniu do systemu zakresu dostępnych dla danego użytkownika danych i dopuszczalnych operacji.
2. Każdy z użytkowników systemu posiada własny identyfikator.
3. Ustanowione hasło dostępu, w sposób poufny ASI przekazuje użytkownikowi.
4. Hasło ustanowione podczas przyznawania uprawnień użytkownik jest zobowiązany zmienić na indywidualne podczas pierwszego logowania się w systemie informatycznym.
5. Użytkownik ma prawo do wykonywania w systemie tylko tych czynności, do których został upoważniony. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako ciężkie naruszenie podstawowych obowiązków pracowniczych.
6. Użytkownik ponosi odpowiedzialność za wszelkie operacje wykonywane przy użyciu jego identyfikatora i hasła lub karty mikroprocesorowej.
7. W przypadku anulowania uprawnień użytkownika jego identyfikator i kartę mikroprocesorową należy niezwłocznie zablokować w systemie oraz unieważnić hasło użytkownika.
8. Za wdrożenie i nadzór nad przestrzeganiem procedury rejestracji uprawnień użytkowników w systemach odpowiedzialny jest ASI

§ 4
Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła, lub weryfikacji tożsamości użytkownika przy użyciu karty mikroprocesorowej.
2. Zmiana hasła użytkownika następuje nie rzadziej niż co 30 dni.

3. Identyfikatora użytkownika nie należy zmieniać bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu nie powinien być on przydzielany innej osobie.
4. Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł i ochronę swoich kart mikroprocesorowych.
5. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności, nie wolno ich udostępniać, ani zapisywać w sposób jawny.
6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
7. W sytuacji kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do jego natychmiastowej zmiany.
8. Przy wyborze hasła obowiązują następujące zasady:
   a. minimalna długość hasła – 8 znaków,
   b. właściwa złożoność hasła - litery duże i małe oraz cyfry lub znaki specjalne.
9. Zakazuje się stosowania haseł:
   a. które użytkownik stosował uprzednio (do sześciu haseł wstecz),
   b. będących nazwą użytkownika w jakiejkolwiek formie (np. pisanej dużymi literami),
   c. analogicznych jak identyfikator,
   d. zawierających ogólnie dostępne informacje takie jak: imię, nazwisko, numer rejestracyjny samochodu, numer telefonu, imiona dzieci itp.,
   e. stanowiących wyrazy słownikowe lub przewidywalne sekwencje znaków np. 12345678 lub abcdefgh.
10. W systemach umożliwiających zapamiętanie hasła nie należy korzystać z tego ułatwienia.
11. Powyższe reguły w zakresie haseł dotyczą obowiązków użytkownika systemu niezależnie od istnienia lub nie mechanizmów wymuszających (ułatwiających) ich stosowanie.

§ 5
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1. Przed rozpoczęciem pracy w systemie informatycznym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora i hasła lub identyfikatora i przypisanej do niego karty mikroprocesorowej.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wylogowania z systemu, zablokowania dostępu poprzez zabezpieczony hasłem wygaszacz ekranu lub zablokowanie, wylogowanie sesji użytkownika, np. poprzez użycie kombinacji klawiszy na klawiaturze komputera:
   a. „Ctrl+Alt+Delete" i wybór polecenia „zablokuj ten komputer" lub „wyloguj",
   b. „logo systemu Windows+L" dla zablokowania komputera.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu.

4. Ustawienie monitora podczas pracy powinno uniemożliwić podgląd jakimkolwiek osobom nieupoważnionym.
5. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów.
6. Przypadki stwierdzenia nieprawidłowości w zakresie działania systemu należy zgłaszać do ASI, który po stwierdzeniu przypadku stanowiącego incydent bezpieczeństwa podejmuje działania.
7. Zabronione jest podejmowanie działań mogących stanowić zagrożenie dla systemu, a w tym:
   a. łamanie haseł,
   b. dokonywanie włamań na konta innych użytkowników,
   c. nieprawne uzyskiwanie dostępu do kont administracyjnych,
   d. zakłócanie działania usług,
   e. omijanie i badanie zabezpieczeń (nie dotyczy czynności wykonywanych w ramach audytu, czynności kontrolnych lub testowania wykonywanych przez osoby upoważnione),
   f. doprowadzanie do rozprowadzania wirusów, robaków i koni trojańskich oraz niechcianej poczty,
   g. praca na koncie innego użytkownika.

§ 6
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. W celu zagwarantowania bezpieczeństwa danych przechowywanych w systemie wykonywane są ich kopie zapasowe, tj. kopie bezpieczeństwa oraz archiwalne.
2. Za systematyczne przygotowanie kopii zapasowych odpowiada ASI. W przypadku części aplikacji ich tworzenie odbywa się automatycznie.
3. Bazy danych, oprogramowanie oraz konfiguracja systemów powinny być zabezpieczone w postaci kopii bezpieczeństwa.
4. Należy wykonywać następujące kopie bezpieczeństwa:
   a. przed dokonaniem zmian w konfiguracji systemów lub oprogramowania,
   b. przed dokonaniem zmian w programach (np. zmiana wersji),
   c. zgodnie z przyjętym harmonogramem.
5. Oprócz kopii bezpieczeństwa wykonywane są okresowo kopie archiwalne istotnych dla działalności UMiG danych.
6. Za wdrożenie i nadzór nad stosowaniem zasad i trybu wykonywania kopii zapasowych odpowiedzialny jest ASI.

§ 7

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

I. Kopie zapasowe.
   1. Kopie zapasowe należy przechowywać w warunkach gwarantujących brak dostępu do nich osób nieupoważnionych, tj. w zabezpieczonych pomieszczeniach, w sejfach lub szafach zamykanych na klucz.
   2. W przypadku wykonywania zabezpieczeń długoterminowych lub na nośnikach zewnętrznych, np. zewnętrznych dyskach, płytach CD, DVD nośniki te należy sprawdzać pod kątem ich dalszej przydatności oraz odtwarzalności.
   3. Kopie zapasowe należy usunąć niezwłocznie po upływie okresów przechowywania lub w przypadku ustania ich użyteczności.

II. Elektroniczne nośniki informacji.
   1. Na terenie UMiG Ostroróg dopuszcza się używanie służbowych (szyfrowanych) elektronicznych nośników informacji typu pendrive w celu przenoszenia i archiwizowania danych osobowych.
   2. Należy unikać przechowywania danych osobowych na nośnikach.
   3. Zabronione jest używanie nośników do przenoszenia danych osobowych na prywatne komputery lub inne, prywatne urządzenia mogące służyć do przechowywania danych.
   4. Nośniki, zawierające dane osobowe, powinny być oznaczone w sposób trwały, jednoznaczny i czytelny. Za ich oznaczenie w podległej komórce organizacyjnej odpowiada KKO.
   5. Nośniki, zawierające dane osobowe, podlegają szczególnemu nadzorowi i są przechowywane w pomieszczeniach stanowiących obszar przetwarzania danych osobowych w zamykanych szafach biurowych lub kasetkach.
   6. W przypadku zaistnienia okoliczności uzasadniających konieczność wyniesienia nośnika zawierającego dane osobowe poza obszar przetwarzania danych osobowych jego użytkownik zobowiązany jest do zachowania szczególnej ostrożności i zabezpieczenia (w postaci szyfrowania) nośnika przed dostępem osób nieupoważnionych, utratą lub zniszczeniem.
   7. Nośniki, zawierające dane osobowe, należy transportować w sposób bezpieczny (nie pozostawić ich w miejscach widocznych np. w samochodach).
   8. Nośniki, 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.

§ 8

Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, a także przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

1. Oprogramowanie stosowane, wdrażane, modyfikowane, zakupione w UMiG Ostroróg może pochodzić wyłącznie ze źródeł legalnych i sprawdzonych oraz powinno spełniać wymagania przepisów z zakresu ochrony danych osobowych.
2. Dozwolone jest jedynie uruchamianie oprogramowania związanego merytorycznie z wykonywaną pracą oraz dopuszczonego przez ASI do użytkowania w systemach UMiG .
3. Korzystanie z zasobów informatycznych UMiG poprzez sieć publiczną winno mieć miejsce po zastosowaniu koniecznych systemów zabezpieczeń i mechanizmów ochronnych, w szczególności firewall-i oraz systemu uwierzytelniania użytkowników i szyfrowania danych, a także kompleksowego oprogramowania antywirusowego.
4. Sieć wewnętrzna UMiG odseparowana jest od sieci publicznej za pomocą uaktywnionych firewalli sprzętowych i programowych.
5. Dostęp do sieci wewnętrznej, przy zastosowaniu zasad dopuszczenia do zasobów informatycznych obowiązujących w UMiG mogą posiadać:
   a. pracownicy UMiG Ostroróg ,
   b. osoby lub podmioty, z którymi UMiG współpracuje na podstawie zawartych umów oraz ich pracownicy – w zakresie przewidzianym umową.
6. W celu ochrony systemów przed szkodliwym oprogramowaniem oprogramowanie antywirusowe podlegające systematycznej aktualizacji musi być zainstalowane na każdym stanowisku komputerowym systemu. Za prawidłowość realizacji powyższego obowiązku odpowiada ASI.
7. Sprawdzanie dostępności baz wirusów oprogramowania antywirusowego odbywa się automatycznie. Zaleca się okresowe monitorowanie czy aktualizacja ta przebiega bez zakłóceń.
8. Użytkownicy zobowiązani są do niezwłocznego zgłaszania do ASI każdej stwierdzonej nieprawidłowości dotyczącej profilaktyki antywirusowej (np. braku zainstalowanego oprogramowania antywirusowego, nieaktualności sygnatur wirusów). ASI podejmuje działania mające na celu eliminację nieprawidłowości w zakresie realizacji obowiązku, o którym mowa w ust. 7 powyżej.
9. Programy antywirusowe winny być uaktywnione cały czas podczas pracy danego systemu.
10. Wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, należy sprawdzać pod kątem występowania szkodliwego oprogramowania najnowszą dostępną wersją programu antywirusowego.

11. Każdy użytkownik zobowiązany jest do ochrony przed szkodliwym oprogramowaniem powierzonego mu stanowiska komputerowego.
12. Zabrania się używania elektronicznych nośników informacji niewiadomego pochodzenia.
13. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia.
14. W przypadku stwierdzenia pojawienia się szkodliwego oprogramowania, każdy użytkownik winien zawiadomić ASI o zaistniałym zdarzeniu.
15. W UMiG powinny być przeprowadzane cyklicznie automatyczne skanowania antywirusowe na wszystkich wykorzystywanych komputerach systemów.

§ 9
Udostępnianie danych osobowych.

1. Dane osobowe administrowane w UMiG mogą być udostępniane:
   a. osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa;
   b. innym osobom i podmiotom w przypadku posiadania przez wnioskującego podstaw do legalnego przetwarzania danych.
2. Udostępnienie danych nie może naruszać praw i wolności osób, których dane dotyczą.
3. W przypadku pojawienia się wątpliwości w zakresie możliwości udostępnienia danych osobowych Administrator zasięga opinii IOD.
4. IOD może wydać opinię negatywną udostępnienia danych jeżeli może to naruszyć bezpieczeństwo i ochronę danych zgromadzonych w systemie informatycznym.
5. W celu nadzoru nad udostępnianiem danych osobowych przypadki przekazania danych należy odnotowywać w systemach.
6. Dane udostępnione UMiG przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

§ 10
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1. Przeglądy, konserwacje lub naprawy systemów i nośników wykorzystywanych w UMiG dokonywane są przez osobę upoważnioną do tego typu czynności, w szczególności ASI.
2. Dopuszcza się realizację czynności określonych w ust. 1 przez specjalistyczne firmy świadczące usługi w tym zakresie; w takim przypadku konieczne jest zawarcie stosownej umowy cywilnoprawnej.
3. Umowy w zakresie świadczenia usług teleinformatycznych wiążące się z przetwarzaniem danych osobowych powinny być traktowane jako powierzenie przetwarzania danych osobowych.

4. Pracownicy firm świadczących usługi, o których mowa w ust. 2 powyżej wykonują zlecone zadania tylko za zgodą ASI, lub innego uprawnionego pracownika UMiG i pod jego nadzorem.
5. W przypadku zdalnego dostępu do komputera (np. w celu wykonywania czynności serwisowych na komputerze) użytkownik komputera musi potwierdzić przejęcie pulpitu komputera oraz nadzorować wszelkie czynności wykonywane przez ASI lub osobę przejmującą pulpit komputera, której zostały zlecone stosowne działania.
6. Przeglądy i konserwacje wykonywane są cyklicznie oraz w przypadku pojawienia się usterki lub awarii systemów informatycznych.
7. Przeglądy mają na celu weryfikację elementów systemu informatycznego i poprawności ich funkcjonowania.
8. Konserwacje mają na celu utrzymanie systemu.
9. Szczegółowy harmonogram i zakres czynności wynikających z przeglądu i konserwacji dla każdego systemu ustala ASI.

§ 11
Przetwarzanie danych osobowych na komputerach przenośnych.

1. Za bezpieczeństwo komputerów przenośnych odpowiedzialni są ich użytkownicy.
2. W sytuacji przetwarzania danych osobowych, przez pracowników UMiG na komputerach przenośnych poza obszarem przetwarzania wskazanym w PODO, odpowiedzialni za ich bezpieczeństwo są ich użytkownicy i są zobowiązani chronić dane przed dostępem do nich osób nieupoważnionych.
3. Komputery przenośne po zakończonej pracy winny być przechowywane przez użytkownika w warunkach zapewniających ich bezpieczeństwo.
4. W przypadku korzystania z komputerów przenośnych poza obszarem przetwarzania należy używać ich w sposób uniemożliwiający odczyt danych z ekranu przez osoby postronne.
5. Podczas transportu komputerów przenośnych wynoszonych poza obszar przetwarzania danych osobowych należy zapewnić ich bezpieczeństwo tj. nie należy ich pozostawiać bez nadzoru w samochodzie (lub innym miejscu). Muszą one być przewożone jako bagaż podręczny.
6. Należy unikać przechowywania na komputerach przenośnych danych osobowych.
7. Komputery przenośne muszą być wyposażone w uaktywniony firewall programowy.
8. W przypadku przetwarzania danych osobowych na komputerach przenośnych baza danych osobowych powinna być szyfrowana, zabezpieczona odpowiednim hasłem.

§ 12
Przetwarzanie danych osobowych na urządzeniach przenośnych, innych niż komputery.

1. Pracownicy korzystający z teleinformatycznych urządzeń przenośnych, tj. m.in. telefonów służbowych, tabletów, aparatów fotograficznych, kamer wideo, są zobowiązani chronić dane osobowe zawarte w pamięci tych urządzeń przed dostępem osób nieupoważnionych.

2. Wszelkie dane osobowe wprowadzone do pamięci urządzeń przenośnych powinny być usunięte przed zdaniem urządzenia do właściwej komórki organizacyjnej. Osobą właściwą do ich usunięcia jest pracownik lub funkcjonariusz korzystający z danego urządzenia. W przypadku trudności technicznych przy usuwaniu danych osobowych należy kontaktować się z SIŁ.

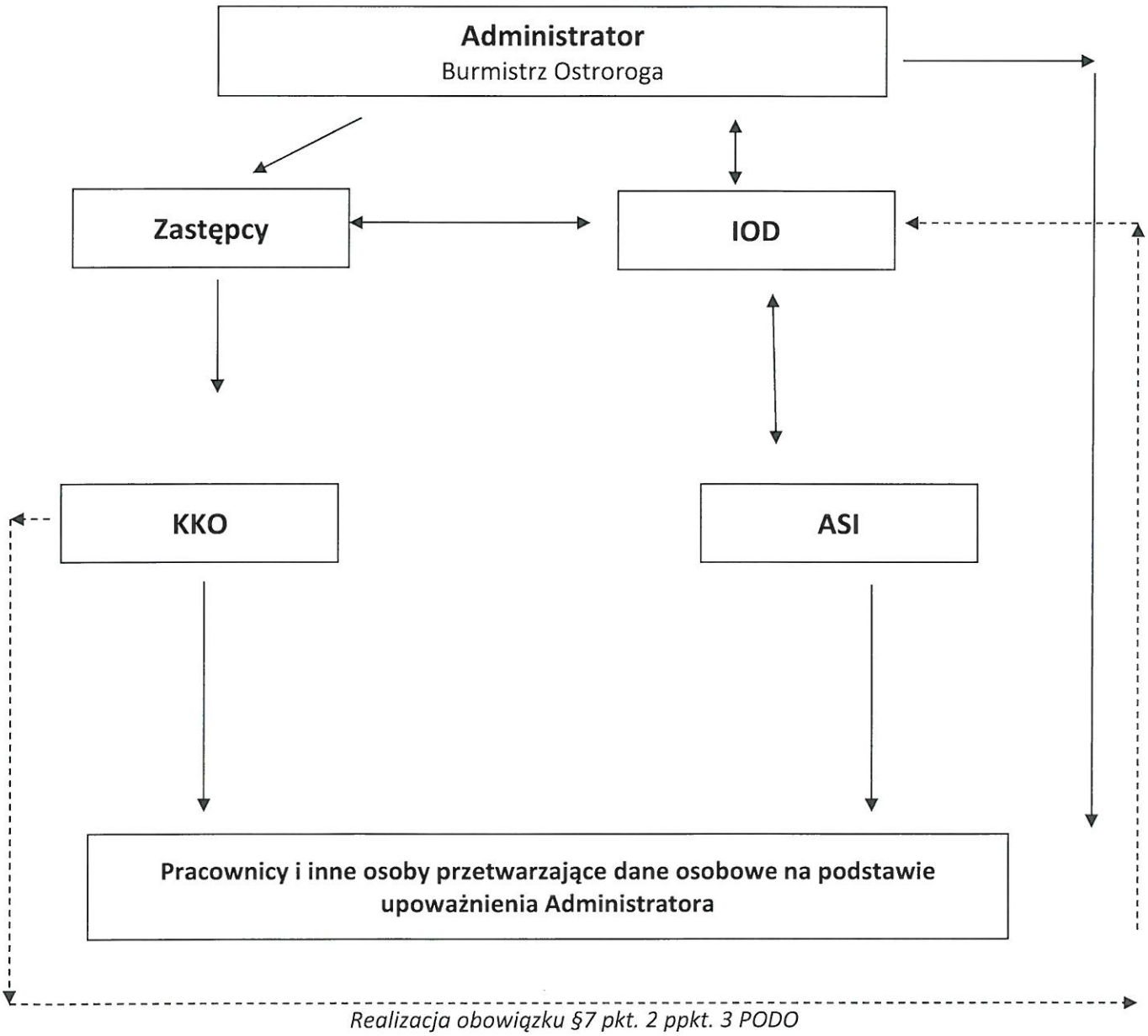
3. Kontakt z serwisami zewnętrznymi, dotyczący użytkowanego sprzętu, możliwy jest tylko za pośrednictwem SIŁ lub za zgodą ASI.

4. W treści informacji o przyznaniu pracownikowi urządzenia powinny znaleźć się wskazania w zakresie ochrony danych osobowych przetwarzanych przy jego pomocy.

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 6
do Polityki Ochrony Danych Osobowych
w UMiG w Ostrorogu

Struktura zarządzania przetwarzaniem danych osobowych oraz ich bezpieczeństwem



BURMISTRZ
dr Sławomir Szałata

Załącznik nr 6b do polityki ochrony danych osobowych

Informacja dla pracownika Urzędu Miasta i Gminy Ostroróg

(Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą)

Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Administrator - Burmistrz Miasta i Gminy Ostroróg informuję, iż:

1. Pani/ Pana dane osobowe oraz dane osobowe członków Pani/Pana rodziny przetwarzane są w Urzędzie Miasta i Gminy Ostroróg, ul. Wroniecka 14, 64-560 Ostroróg.
2. Funkcję Inspektora Ochrony Danych (IOD) pełni wyznaczony pracownik Urzędu, kontakt telefoniczny: 61 29 31 717, mail: iod@ostrorog.eu
1. Celem przetwarzania Pani / Pana danych osobowych przez UMiG Ostroróg jest wypełnienie obowiązków wynikających z przepisów prawa, w szczególności: a) kodeks pracy, b) ustawa o podatku dochodowym od osób fizycznych c) ustawa o systemie ubezpieczeń społecznych; d) ustawa o powszechnym ubezpieczeniu zdrowotnym; e) ustawa o zakładowym funduszu świadczeń socjalnych, f) inne obowiązujące pracodawcę przepisy prawa.
2. Odbiorcami Pani / Pana danych osobowych są: lekarz medycyny pracy; właściwy urząd skarbowy oraz zakład ubezpieczeń społecznych, podmiot świadczący usługi z zakresu bhp oraz inne podmioty z którymi Administrator zawarł umowy cywilno-prawne.
3. Pani/Pana dane osobowe będą przechowywane w UMiG w Ostrorogu zgodnie z przepisami wynikającymi z kodeksu pracy oraz zgodnie z jednolitym rzeczowym wykazem akt (instrukcja kancelaryjna).
4. Posiada Pani/Pan prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych.
5. Podanie przez Panią / Pana danych osobowych jest warunkiem zawarcia i trwania umowy o pracę oraz wypełnianie pozostałych obowiązków ciążących na pracodawcy. Jest Pani / Pan zobowiązana/ny do podania danych osobowych, a ich niepodanie uniemożliwi Pani / Panu świadczenie pracy w Urzędzie.
6. Posiada Pani/Pan prawo do: a) żądania od administratora dostępu do swoich danych osobowych; b) prawo do sprostowania danych; c) prawo do usunięcia danych („prawo do bycia zapomnianym"), d) prawo ograniczenia przetwarzania; e) prawo do wniesienia sprzeciwu wobec przetwarzania; f) prawo do przenoszenia danych, g) prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, h) prawo do wycofania zgody na dalsze przetwarzania wysyłając stosowne powiadomienie.

Oświadczenie pracownika

Oświadczam, że w dniu ..... zapoznałam/-em się z przekazaną mi powyżej informacją dotyczącą zasad, potrzeb gromadzenia i przetwarzania przez UMiG Ostroróg moich danych osobowych oraz danych osobowych członków mojej rodziny w celu wypełnienie przez pracodawcę obowiązków wynikających z przepisów prawa.

.....
(czytelny podpis – imię i nazwisko osoby składającej oświadczenie)

*)niepotrzebne skreślić

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 7
do Polityki Ochrony Danych Osobowych w UMiG w Ostrorogu

.....
(pieczątka nagłówkowa)

UPOWAŻNIENIE
do przetwarzania danych osobowych

Na podstawie art. 29 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679, upoważniam Panią/Pana .....
do przetwarzania danych osobowych w systemie informatycznym/nieinformatycznym[1)] w zakresie zasobów przetwarzanych w ramach pełnionych obowiązków pracowniczych/służbowych/wynikających z zawartej umowy zlecenie/praktyk/stażu[2)] .

Data nadania ..... Data ustania .....

Identyfikator w systemie .....

Wyżej wymieniona osoba została dopuszczona do przetwarzania danych osobowych w zakresie określonym w ogólnym rozporządzeniu o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679 oraz procedurach i instrukcjach, obowiązujących w UMiG w Ostrorogu, w sprawie ochrony danych osobowych.

.....
(podpis Administratora lub osoby upoważnionej do nadawania i podpisywania upoważnień w jego imieniu)

.....
(data i podpis osoby upoważnionej)

OBJAŚNIENIA.
1) *właściwe podkreślić,*
2) *właściwe podkreślić lub wstawić inny zakres obowiązków,*

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 8
do Polityki Ochrony Danych Osobowych
w UMiG w Ostrorogu

.....
(pieczątka nagłówkowa)

UPOWAŻNIENIE
do udzielania oraz cofania upoważnień do przetwarzania danych osobowych

W związku z art. 24 ust. 1 i art. 29 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679, oraz zgodnie z zapisami Polityki Ochrony Danych Osobowych w UMiG w Ostrorogu upoważniam Panią/Pana .....,

.....,

(stanowisko)

do udzielania oraz cofania upoważnień do przetwarzania danych osobowych w[1)] .....,

dla osób uczestniczących w przetwarzaniu tych danych w .....

.....
(podpis Administratora)

OBJAŚNIENIA.

1) *Podać nazwę zasobu, zbioru danych osobowych lub systemu informatycznego, w którym będą przetwarzane dane osobowe.*

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 9
do Polityki Ochrony Danych Osobowych
w UMiG w Ostrorogu

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał(a) dostęp w związku z wykonywaniem prac na rzecz UMiG w Ostrorogu.

Zobowiązuję się przestrzegać polityk, instrukcji, regulaminów i procedur obowiązujących w UMiG w Ostrorogu dotyczących ochrony danych osobowych, w szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał(a) danych osobowych ze zbiorów UMiG w Ostrorogu.

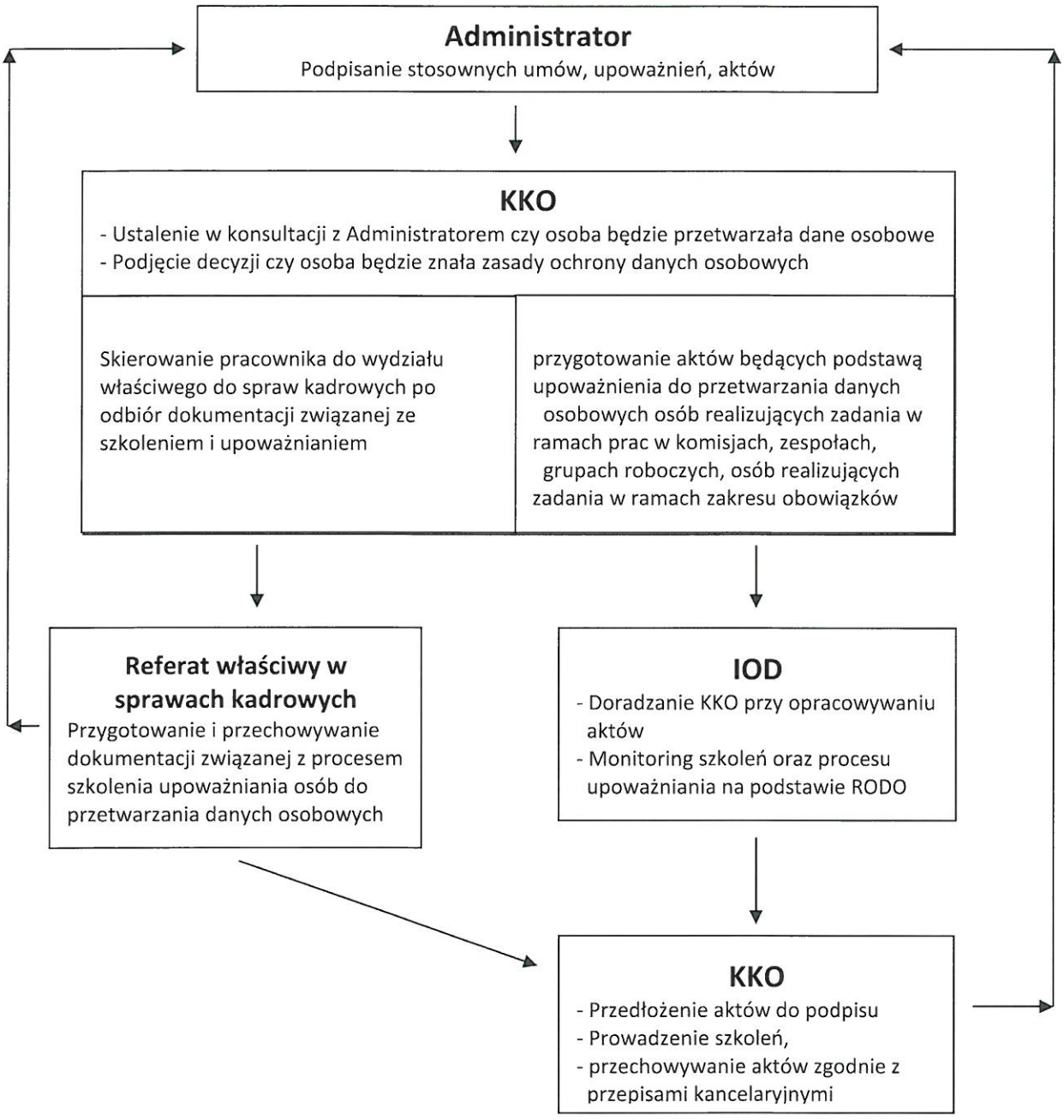
Oświadczam, że zostałam(em) zapoznana(y) z przepisami ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679, właściwymi przepisami z zakresu ochrony danych osobowych, w tym informacjami o grożącej odpowiedzialności karnej, a także z procedurami i instrukcjami obowiązującymi w zakresie ochrony danych osobowych w UMiG w Ostrorogu.

.....
(data i czytelny podpis osoby upoważnionej do przetwarzania danych osobowych)

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 10
do Polityki Ochrony Danych Osobowych
w UMiG w Ostrorogu

Struktura organizacyjna związana z polecaniem osobom przetwarzania danych osobowych[1)]



Objaśnienia.
[1)]Przedstawiona struktura jest tylko materiałem pomocniczym do analizy zapisów §6 PODO

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 11
do Polityki Ochrony Danych Osobowych
w UMiG w Ostrorogu

WZORY ZAPISÓW UMOWY DOTYCZĄCEJ POWIERZENIA CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:

Urzędem Miasta i Gminy Ostroróg

_____

_____

zwana w dalszej części umowy „Administratorem"

reprezentowana przez: _____

oraz

(dane podmiotu który umowę zawiera, w szczególności: firma spółki, siedziba, adres, oznaczenie sądu rejestrowego, w którym przechowywana jest dokumentacja spółki oraz numer pod którym spółka jest wpisana do rejestru; NIP. W przypadku podmiotów prowadzących działalność gospodarczą imię nazwisko adres zamieszkania osoby fizyczne, PESEL, firma pod jaką działalność jest prowadzona oraz adres głównego miejsca wykonywania działalności)

zwana w dalszej części umowy „Podmiotem Przetwarzającym"

reprezentowana przez:

_____

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi Przetwarzającemu w trybie art. 28 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu

Europejskiego i Rady (UE) 2016/679, zwanego dalej Rozporządzeniem, dane osobowe do przetwarzania na zasadach i w celu określonym w niniejszej umowie.

2. Podmiot Przetwarzający zobowiązuje się przetwarzać:
   a) powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
   b) powierzone mu na podstawie umowy dane osobowe .....[1)]
   .....[2)]
   wyłącznie w celu .....
   c) powierzone mu na podstawie umowy dane osobowe .....[3)]

3. Podmiot Przetwarzający oświadcza, że stosuje środki techniczne i organizacyjne spełniające wymogi Rozporządzenia i chroniące prawa osób, których dane dotyczą.

§ 2

Sposób wykonania umowy w zakresie przetwarzania danych osobowych

1. Podmiot Przetwarzający:
   a) zobowiązuje się przy przetwarzaniu danych osobowych podjąć wszelkie środki wymagane na mocy art. 32 Rozporządzenia, zapewniające adekwatny stopień bezpieczeństwa odpowiadający ryzyku określonym w tym artykule,
   b) zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji umowy,
   c) zapewnia, ze osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub podlegają ustawowemu obowiązkowi zachowania tajemnicy, zarówno w trakcie trwania zatrudnienia w Podmiocie Przetwarzającym jak i po jego ustaniu,
   d) może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora,
   e) po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych .....[4)] wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych,
   f) uwzględniając charakter przetwarzania oraz dostępne mu informacje pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32-36 Rozporządzenia,
   g) po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi, ale nie później niż w ciągu 24 godzin,

h) biorąc pod uwagę charakter przetwarzania, w miarę możliwości oraz przy uwzględnieniu ograniczeń, o których mowa w art. 23 Rozporządzenia pomaga Administratorowi w niezbędnym zakresie wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia,
i) udostępnia Administratorowi niezwłocznie wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia oraz niniejszej umowie,
j) umożliwia Administratorowi lub osobie upoważnionej przez Administratora przeprowadzenie kontroli w postaci audytów, inspekcji, dotyczących oceny czy środki zastosowane przez Podmiot Przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia niniejszej umowy; działania, o których mowa powinny nastąpić w godzinach pracy Podmiotu Przetwarzającego nie później niż w ciągu 24 godzin od powzięcia o nich wiadomości lub w innym terminie wskazanym przez Administratora.
k) Zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora lub nie dłuższym niż 7 dni.

2. Jeżeli do wykonania w imieniu Administratora konkretnych czynności przetwarzania danych osobowych Podmiot Przetwarzający korzysta z usług podwykonawców to:
   a) podwykonawca winien spełniać te same gwarancje i obowiązki w zakresie ochrony danych osobowych jakie zostały nałożone na Podmiot Przetwarzający w niniejszej umowie,
   b) jeżeli podwykonawca nie wywiąże się ze spoczywających na nim obowiązków ochrony danych osobowych, pełną odpowiedzialność za ten stan wobec Administratora ponosi Podmiot Przetwarzający.

3. Przekazanie powierzonych Podmiotowi Przetwarzającemu danych do państwa trzeciego lub organizacji międzynarodowej może nastąpić jedynie na pisemne polecenie Administratora chyba, że obowiązek taki nakłada na Podmiot Przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot Przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania Podmiot Przetwarzający informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

4. Administrator zgodnie z art. 28 ust. 3 lit h) Rozporządzenia ma prawo kontroli poprzez przeprowadzanie audytów, w tym inspekcji, czy środki zastosowane przez Podmiot Przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia niniejszej umowy.

OBJAŚNIENIA.

1) *Należy podać rodzaj danych: dane osobowe zwykłe lub/i dane osobowe szczególnych kategorii.*
2) *Należy podać kategorię lub kategorie osób, których dane dotyczą, np.:*
   - *pracownicy administratora,*
   - *osoby zatrudnione na innej podstawie niż stosunek pracy,*
   - *osoby uczące się u Administratora,*
   - *osoby biorące udział w konkursie ..... (podać nazwę konkursu),*
   - *osoby realizujące usługi na rzecz Administratora,*
   - *kontrahenci.*

3) Należy podać czas trwania przetwarzania

4) Należy wstawić jedno z określeń:
   - *usuwa,*
   -*zwraca Administratorowi.*

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 12
Do Polityki Bezpieczeństwa Danych Osobowych
w UMiG w Ostrorogu

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679 informujemy, że:

1. Administratorem przetwarzającym Pani(a) dane osobowe jest Burmistrz Miasta i Gminy Ostroróg, z siedzibą w Ostrorogu, ul. Wroniecka 14.
2. W UMiG Ostroróg wyznaczony został Inspektor Ochrony Danych, mail: .....
3. Pani(a) dane osobowe będą przetwarzane w celu .....
   na podstawie .....
4. Odbiorcą Pani(a) danych osobowych są .....
5. Pani(a) dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.[4)]
6. Pani(a) dane osobowe będą przechowywane przez okres .....
7. Posiada Pani(-) prawo żądania dostępu do treści swoich danych, prawo ich sprostowania, usunięcia ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania, prawo do przenoszenia danych, prawo do cofnięcia zgody na przetwarzanie w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
8. Posiada Pani(-) prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych jeżeli uzna Pani (-), że przetwarzanie narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
9. Podanie przez Panią(a) danych osobowych jest wymogiem ustawowym/umownym/warunkiem zawarcia umowy[1)] . Jest Pani(-) zobowiązany do ich podania *(przyp. lub nie jest Pani(-) zobowiązany)* , a konsekwencją niepodania danych osobowych będzie .....
10. Przetwarzanie podanych przez Panią(-) danych osobowych nie będzie podlegało zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu, o którym mowa w art. 22 ust. 1 i 4 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

OBJAŚNIENIA.
1) niepotrzebne skreślić

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 13
do Polityki Ochrony Danych Osobowych
w UMiG w Ostrorogu

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Zgodnie z art. 6 ust. 1 lit. a ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679 wyrażam zgodę, na przetwarzanie moich danych osobowych .....[1)], przez Burmistrza Miasta i Gminy Ostroróg w celu .....
.....

Zgodnie z art. 7 ust. 3 wyżej wskazanego Rozporządzenia zgoda udzielona na przetwarzanie danych osobowych może być wycofana w formie oświadczenia na piśmie w dowolnym czasie, nie wpływa to jednak na zgodność przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

.....
(miejscowość i data)

.....
(podpis osoby wyrażającej zgodę)

OBJAŚNIENIA.

1) wskazać o jakie dane osobowe chodzi.

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 14
o Polityki Ochrony Danych Osobowych
w UMiG w Ostrorogu

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

§ 1

Osoby zobowiązane do ochrony danych osobowych

1. Osobami odpowiedzialnymi za ochronę danych osobowych, zgodnie z właściwością, są :
   a) Burmistrz,
   b) Zastępcy Burmistrza,
   c) IOD,
   d) ASI,
   e) KKO,
   f) osoby upoważnione do przetwarzania danych osobowych,
   g) osoby, które nie przetwarzają danych osobowych, ale w ramach czynności poznały sposoby ich zabezpieczania.

§ 2

Obowiązki osób zobowiązanych do ochrony danych osobowych w sytuacji naruszenia ochrony danych osobowych

1. Każdy zobowiązany do ochrony danych osobowych, zwany dalej Zobowiązanym, jeśli stwierdzi lub podejrzewa naruszenie zabezpieczenia danych osobowych, powinien niezwłocznie poinformować o tym:
   a) właściwego KKO, którego obowiązkiem jest poinformowanie o naruszeniu Administratora lub osoby zastępującej Burmistrza, ABS i IOD.
   b) bezpośrednio Administratora w sytuacjach szczególnych, do których zaliczyć można podejrzenie braku bezstronności osób wskazanych w § 2 pkt. 1 lit. a).
2. W celu poinformowania Administratora stosuję się wzór stanowiący załącznik nr 1 do do niniejszej Instrukcji.
3. Informację o naruszeniu Administrator powinien niezwłocznie przekazać do IOD w celu umożliwienia mu realizacji jego obowiązków.
4. Zobowiązany, który stwierdził lub podejrzewa naruszenie zabezpieczenia danych osobowych, oprócz obowiązku wymienionego w § 2 pkt. 1 powinien:

a) powstrzymać się od wykonywania pracy lub jakichkolwiek czynności mogących spowodować zatarcie śladów lub dowodów naruszenia,
b) podjąć, odpowiednie do zaistniałej sytuacji działania niezbędne do zapobieżenia dalszym zagrożeniom, które mogą skutkować naruszeniem danych osobowych.

5. Administrator, a w przypadku jego nieobecności osoba wyznaczona przez Burmistrz, po stwierdzeniu lub uzyskaniu informacji o naruszeniu ochrony danych osobowych powinien:
   a) przystąpić do identyfikacji rodzaju zdarzenia, a w szczególności do określenia skali zniszczeń, dostępu do danych osobowych itp.,
   b) podjąć odpowiednie kroki w celu zminimalizowania szkód i rozmiarów zdarzenia oraz zabezpieczenia przed usunięciem śladów zdarzenia,
   c) osobiście lub polecić IOD w terminie 72 godzin przesłać do właściwego Organu Nadzorczego zgłoszenie naruszenia ochrony danych osobowych jeżeli skutkowało ono ryzykiem naruszenia praw i wolności osób fizycznych;
   d) osobiście lub polecić IOD bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą o naruszeniu jeżeli skutkowało ono ryzykiem naruszenia praw i wolności osób fizycznych; postępowanie to powinno być zgodne z art. 34 RODO,
6. IOD jest zobowiązany zarejestrować zdarzenie; wzór „Rejestru naruszeń ochrony danych osobowych w UMiG w Ostrorogu" stanowi załącznik nr 2 do niniejszej Instrukcji.
7. Administrator, czynności o których mowa w § 2 pkt. 3 lit. b), c), w sytuacjach szczególnych, takich jak konieczność zgłoszenia naruszenia ochrony danych osobowych do właściwego Organu Nadzorczego, może dokumentować wykorzystując załączniki do PODO określone w rozdziale XIV Polityki „Monitorowanie przestrzegania RODO, innych właściwych przepisów o ochronie danych osobowych oraz PODO"; sporządzeniem tej dokumentacji powinien zająć się wskazany pracownik Administratora, a w sytuacjach szczególnych IOD; sprawozdanie z okoliczności zdarzenia osoba sporządzająca przedkłada Burmistrzowi.
8. W przypadku zdarzenia mającego związek z systemem informatycznym ASI zobowiązany jest do:
   a) szczegółowej analizy systemu w celu potwierdzenia lub wykluczenia faktu naruszenia,
   b) wygenerowania, wydrukowania wszystkich możliwych dokumentów, raportów lub zestawień, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrując je
   c) datą i podpisem,
   d) fizycznego odłączenia urządzenia, segmentu sieci, które mogły umożliwiać dostęp do bazy danych osobowych osobie nieupoważnionej,
   e) wylogowania użytkownika podejrzewanego o naruszenie ochrony danych osobowych,

f) zmiany haseł na konta, poprzez które uzyskano nielegalny dostęp,

g) przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, przywrócenia jej z ostatniej kopii awaryjnej z zachowaniem środków ostrożności przed ponownym dostępem tą samą drogą przez osobę nieupoważnioną,

9. ASI o podjętych działaniach powinien niezwłocznie poinformować Administratora.

10. Wszyscy zobowiązani mają obowiązek udzielić wszelkiej niezbędnej pomocy przy realizacji zadań przez IOD.

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 1
do Instrukcji Postępowania w Sytuacji Naruszenia Ochrony Danych Osobowych

WZÓR ZGŁOSZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH DO WŁAŚCIWEGO ORGANU NADZORCZEGO

.....
(pieczątka nagłówkowa)
.....
(znak sprawy)

.....
(dane adresowe właściwego organu nadzorczego)

Zgodnie z art. 33 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady (UE) 2016/679 zgłaszam fakt naruszenia ochrony danych osobowych w Urzędzie Miasta i Gminy Ostroróg, z siedzibą przy ul. Wroniecka 14.

Naruszenie zostało zgłoszone do Administratora w dniu ..... o godzinie ..... przez .....[1)]. Poniżej przedstawiono informacje wynikające z art. 33 ust. 2 wskazanego wyżej Rozporządzenia.

1. Opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczby wpisów danych osobowych, których dotyczy naruszenie.
   .....

2. Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji.
   .....

3. Opis możliwych konsekwencji naruszenia ochrony danych osobowych.
   .....

4. Opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.
   .....

.....
(Podpis Administratora lub osoby upoważnionej

OBJAŚNIENIA.

1) *W zależności od okoliczności podać zamiennie: „Naruszenie zostało wykryte przez Administratora w dniu ..... o godzinie .....”*

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 2
do Instrukcji Postępowania w Sytuacji Naruszenia Ochrony Danych Osobowych

.....
(pieczątka nagłówkowa)

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH
w UMiG Ostroróg

Lp.	Data i godzina zgłoszenia IOD faktu naruszenia	Imię i nazwisko osoby zgłaszającej naruszenie	Okoliczności naruszenia	Skutki naruszenia	Opis podjętych działań zaradczych	Decyzja Administratora o zgłoszeniu naruszenia właściwemu organowi nadzorczemu	Decyzja Administratora o powiadomieniu o naruszeniu osoby, której dane dotyczą	Podpis Administratora
1.	2.	3.	4.	5.	6.	7.	8.	9.

BURMISTRZ
dr Sławomir Szałata

Załącznik Nr 15
do Polityki Ochrony Danych Osobowych
w UMiG w Ostrorogu

Pierwotny poziom ryzyka (Rp) obliczany jest według wzoru:
Rp = P*(Sd+Si+Sp)

Rp ∈ (0;48)

P – prawdopodobieństwo materializacji zagrożenia, P ∈ {0,1,2,3,4}

gdzie:

0	– zdarzenie nieprawdopodobne(zagrożenie nie występuje)
1	– zdarzenie prawie nieprawdopodobne
2	– zdarzenie mało prawdopodobne
3	– zdarzenie wysoce prawdopodobne
4	– zdarzenie niemal pewne

Sd – skutki dla dostępności informacji, Sd ∈{0,1,2,3,4}
Si – skutki dla integralności informacji, Si ∈{0,1,2,3,4}
Sp – skutki dla poufności informacji, Sp ∈{0,1,2,3,4}

gdzie:

0	– zdarzenie nie powoduje skutku (brak podatności)
1	– zdarzenie wywołuje niewielki skutek
2	– zdarzenie wywołuje znaczący skutek
3	– zdarzenie wywołuje bardzo znaczący skutek
4	– zdarzenie wywołuje skutek katastrofalny

Końcowy poziom ryzyka (Rk) obliczany jest według wzoru:
Rk = P×(Sd/ΣCd+Si/ΣCi+Sp/ΣCp)

Rk ∈ (0;48)

wysokie	50%
progowe	40%
akceptowalne	20%
niskie	

C – skuteczność zabezpieczenia, Cd;Ci;Cp∈ {1,2,3,4}

gdzie:

1	brak zabezpieczenia
2	zabezpieczenie ogranicza poziom ryzyka
3	zabezpieczenie w istotny sposób ogranicza poziom ryzyka
4	zabezpieczenie w bardzo istotny sposób ogranicza poziom ryzyka

Zasoby
Sprzęt/Sieć/Nośniki
Oprogramowanie
Personel/Organizacja
Siedziba
Dokumenty papierowe

Kategorie zagrożeń
Brak
Fizyczne
Organizacyjne
Techniczne
Personel

Akceptuję ryzyka

.....dnia.....2018r

Istotność: 1

Lp.	Nazwa zagrożenie	Prawdopodobieństwo wystąpienia zagrożenia (pobierane automatycznie)	Wpływ zagrożenia na utratę dostępności do informacji	Wpływ zagrożenia na utratę integralności informacji	Wpływ zagrożenia na utratę poufności informacji	Pierwotny poziom ryzyka	Zabezpieczenie 1	Zabezpieczenie 2	Zabezpieczenie 3	Cd	Ci	Cp	Cd	Ci	Cp	Końcowy poziom ryzyka	Wnioski
1	Pożar	1	4	4	4	0,25	Brak	Brak	Brak	1	1	1	1	1	1	0,25	
2	Zalanie	1	4	1	0	0,1041667	Brak	Brak	Brak	1	1	1	1	1	1	0,1041667	
3	Katastrofa budowlana, Poważny wypadek	1	4	1	4	0,1875	Brak	Brak	Brak	1	1	1	1	1	1	0,1875	
4	Zniszczenie urządzeń lub nośników	2	4	1	0	0,2083333	Brak	Brak	Brak	1	1	1	1	1	1	0,2083333	
5	Zjawiska sejsmiczne (trzęsienie ziemi, tąpnięcia)	0	4	1	4	0	Brak	Brak	Brak	1	1	1	1	1	1	0	
6	Zjawiska wulkaniczne	0	4	1	4	0	Brak	Brak	Brak	1	1	1	1	1	1	0	
7	Zjawiska pogodowe (np. piorun, huragan)	1	1	0	0	0,0208333	Brak	Brak	Brak	1	1	1	1	1	1	0,0208333	
8	Powódź	0	4	1	4	0	Brak	Brak	Brak	1	1	1	1	1	1	0	
9	Awaria systemu klimatyzacji	2	1	0	0	0,0416667	Brak	Brak	Brak	1	1	1	1	1	1	0,0416667	
10	Utrata mediów - woda, prąd	4	2	2	0	0,3333333	Brak	Brak	Brak	1	1	1	1	1	1	0,3333333	
11	Utrata możliwości korzystania złączy telefonicznych lu	2	3	0	0	0,125	Brak	Brak	Brak	1	1	1	1	1	1	0,125	
12	Promieniowanie elektromagnetyczne	0	4	4	1	0	Brak	Brak	Brak	1	1	1	1	1	1	0	
13	Szpiegostwo, terroryzm, wandalizm	3	4	2	1	0,4375	Brak	Brak	Brak	1	1	1	1	1	1	0,4375	
14	Wykorzystanie promieniowania ujawniającego (w tym	1	0	0	4	0,0833333	Brak	Brak	Brak	1	1	1	1	1	1	0,0833333	
15	Kradzież nośników lub dokumentów	1	4	2	2	0,1666667	Brak	Brak	Brak	1	1	1	1	1	1	0,1666667	
16	Kradzież urządzenia	1	4	3	1	0,1666667	Brak	Brak	Brak	1	1	1	1	1	1	0,1666667	
17	Odtworzenie z powtórnie wykorzystanych lub wyrzuco	1	4	3	1	0,1666667	Brak	Brak	Brak	1	1	1	1	1	1	0,1666667	
18	Ujawnienie danych	3	0	0	4	0,25	Brak	Brak	Brak	1	1	1	1	1	1	0,25	
19	Dane z niewiarygodnych źródeł	1	2	4	1	0,1458333	Brak	Brak	Brak	1	1	1	1	1	1	0,1458333	
20	Przejęcie kontroli nad urządzeniem / oprogramowanie	2	2	2	1	0,2083333	Brak	Brak	Brak	1	1	1	1	1	1	0,2083333	
21	Sfałszowanie oprogramowania	2	4	4	1	0,375	Brak	Brak	Brak	1	1	1	1	1	1	0,375	
22	Wyłudzenie, fałszowanie dokumentów - nośników kluc	2	4	4	1	0,375	Brak	Brak	Brak	1	1	1	1	1	1	0,375	
23	Awaria urządzenia	3	4	4	1	0,5625	Brak	Brak	Brak	1	1	1	1	1	1	0,5625	
24	Niewłaściwe funkcjonowanie urządzeń	3	4	4	1	0,5625	Brak	Brak	Brak	1	1	1	1	1	1	0,5625	
25	Przeciążenie systemu informacyjnego	3	4	4	1	0,5625	Brak	Brak	Brak	1	1	1	1	1	1	0,5625	
26	Niewłaściwe funkcjonowanie oprogramowania	2	4	4	1	0,375	Brak	Brak	Brak	1	1	1	1	1	1	0,375	
27	Naruszenie zdolności utrzymania systemu informacyj	2	4	4	1	0,375	Brak	Brak	Brak	1	1	1	1	1	1	0,375	
28	Nieautoryzowane użycie urządzeń	2	2	2	4	0,3333333	Brak	Brak	Brak	1	1	1	1	1	1	0,3333333	
29	Nieuprawnione kopiowanie oprogramowania	2	4	4	1	0,375	Brak	Brak	Brak	1	1	1	1	1	1	0,375	
30	Użycie fałszywego lub skopiowanego oprogramowani	2	4	4	1	0,375	Brak	Brak	Brak	1	1	1	1	1	1	0,375	
31	Zniekształcenie danych	2	4	1	1	0,25	Brak	Brak	Brak	1	1	1	1	1	1	0,25	
32	Nielegalne przetwarzanie danych	2	4	1	1	0,25	Brak	Brak	Brak	1	1	1	1	1	1	0,25	
33	Podsłuch	0	4	3	1	0	Brak	Brak	Brak	1	1	1	1	1	1	0	
34	Przełamanie zabezpieczeń	2	4	3	1	0,3333333	Brak	Brak	Brak	1	1	1	1	1	1	0,3333333	
35	Błędy, pomyłki użytkowników i administratorów	4	4	4	1	0,75	Brak	Brak	Brak	1	1	1	1	1	1	0,75	
36	Zaniedbania użytkowników i administratorów	4	4	4	4	1	Brak	Brak	Brak	1	1	1	1	1	1	1	
37	Fałszowanie praw	2	4	3	1	0,3333333	Brak	Brak	Brak	1	1	1	1	1	1	0,3333333	
38	Odmowa działania	4	3	1	1	0,4166667	Brak	Brak	Brak	1	1	1	1	1	1	0,4166667	
39	Niedostępność pracowników (choroba ważnych osób,	4	4	3	1	0,6666667	Brak	Brak	Brak	1	1	1	1	1	1	0,6666667	
40	Błąd użytkowania dokumentacji	2	4	3	4	0,4583333	Brak	Brak	Brak	1	1	1	1	1	1	0,4583333	
41	Źle przypisane uprawnienia	2	4	1	4	0,375	Brak	Brak	Brak	1	1	1	1	1	1	0,375	
42	Złośliwe oprogramowanie	3	4	4	4	0,75	Brak	Brak	Brak	1	1	1	1	1	1	0,75	
43	Ujawnienie w sieci internet	1	0	0	4	0,0833333	Brak	Brak	Brak	1	1	1	1	1	1	0,0833333	
44	Zbyt duże gromadzenie informacji	2	1	1	3	0,2083333	Brak	Brak	Brak	1	1	1	1	1	1	0,2083333	
45	Celowe skasowanie danych	1	4	4	0	0,1666667	Brak	Brak	Brak	1	1	1	1	1	1	0,1666667	
46	Przypadkowe skasowanie danych	4	4	4	0	0,6666667	Brak	Brak	Brak	1	1	1	1	1	1	0,6666667	
47	Brak lub niepoprawne kopie bezpieczeństwa	3	4	4	0	0,5	Brak	Brak	Brak	1	1	1	1	1	1	0,5	
48	Aktualizacja oprogramowania	4	3	3	4	0,8333333	Brak	Brak	Brak	1	1	1	1	1	1	0,8333333	

Szacowania dokonał zespół w składzie:

1. .....
(imię, nazwisko, stanowisko lub funkcja)

2. .....
(imię, nazwisko, stanowisko lub funkcja)

3. .....
(imię, nazwisko, stanowisko lub funkcja)

BURMISTRZ

dr Sławomir Szałata

C:\Users\Tomek\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\DM0C4S2W\załącznik nr 15 arkusz szacowania ryzyka (2)