BURMISTRZ ZAWICHOSTU

Zarządzenie Nr 131 / 2019
Burmistrza Zawichostu
z dnia 07 sierpnia 2019.

w sprawie wprowadzenia Księgi Polityk i Zasad Ochrony Danych Osobowych w Urzędzie Miasta i Gminy Zawichost

Na podstawie art. 24 ust. 1i 2 rozporządzenia Parlamentu Europejskiego i Rady 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)zarządza się, co następuje:

§ 1

Wprowadza się Księgę Polityk i Zasad Ochrony Danych Osobowych w Urzędzie Miasta i Gminy Zawichost jako załącznik nr 1 do niniejszego zarządzenia.

§ 2

Nadzór nad wykonaniem zarządzenia powierza się Sekretarzowi Gminy Zawichost.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ
mgr Katarzyna Kondziołka

BURMISTRZ ZAWICHOSTU

Załącznik do
Zarządzenia Nr 131 / 2019

KSIĘGA POLITYK I ZASAD
OCHRONY DANYCH OSOBOWYCH
W Urzędzie Miasta i Gminy Zawichost

Spis treści

1. Podstawa prawna:

Księga Polityk i Zasad oraz inne dokumenty szczegółowe związane z bezpieczeństwem informacji opierają się na:

1) Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U. UE L.2016.119.1), zwanym w dalszej części RODO.
2) Ustawie z dnia 10 maja 2018 roku o ochronie danych osobowych, zwanym w dalszej części (Dz.U. 2018 poz. 1000) zwaną w dalszej części ODO.
3) Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64 poz. 565).
4) Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012 poz. 526).

1.2. Podstawowe definicje:

1. **Administrator Danych (Administrator)** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
2. **Administrator Systemu Informatycznego (ASI)** – osoba zarządzająca systemem informatycznym, w którym przetwarzane są dane w tym dane osobowe.
3. **Analiza ryzyka** – proces dążący do określenia charakteru i poziomu ryzyka.
4. **Dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
5. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie.
6. **Inspektor Ochrony Danych** – osoba, którą wyznaczył Administrator Danych i powiadomił o tym fakcie Prezesa Urzędu Ochrony Danych Osobowych.
7. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym.
8. **Naruszenie ochrony danych osobowych (incydent ochrony danych)** – 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.
9. **Odbiorca** – 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 Europejskiej lub prawem państwa członkowskiego nie są jednak uznawane za odbiorców. Przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie co celów przetwarzania.
10. **Osoba upoważniona** – osoba posiadająca formalne upoważnienie wydane przez Administratora Danych lub osobę przez niego wyznaczoną.
11. **Podmiot przetwarzający (procesor)** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane w imieniu Administratora Danych.

12. **Przedstawiciel** - oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 RODO do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia.
13. **Przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
14. **Pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
15. **Strona trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający, czy osoby, które z upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe.
16. **System teleinformatyczny** – sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych. System ten tworzy sieć telekomunikacyjną Administratora Danych.
17. **Tajemnica przedsiębiorstwa** – zgodnie z ustawą o zwalczaniu nieuczciwej konkurencji rozumie się „nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich w poufności. Dokumenty oraz informacje w nich zawarte, do których Administrator Danych podpisał umowy o zachowaniu ich w poufności.
18. **Użytkownik** – osoba upoważniona do przetwarzania danych, której przyznano identyfikator i hasło.
19. **Współadministrator** – administrator, który co najmniej z jednym administratorem ustala cele i sposoby przetwarzania danych.
20. **Zbiór danych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

21. **Zgoda osoby, której dane dotyczą** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
22. **Zarządzanie incydentami związanymi z bezpieczeństwem informacji** – procesy wykrywania, raportowania, szacowania, reagowania, podejmowania akcji i wyciągania wniosków z incydentów związanych z bezpieczeństwem informacji.
23. **Zarządzanie ryzykiem** – skoordynowane działania dotyczące kierowania i nadzorowania organizacji w odniesieniu do ryzyka.
24. **Kierownik komórki organizacyjnej** – Kierownik Wydziału/ Referatu.
25. **Pracownik merytoryczny** – pracownik Urzędu Miasta i Gminy Zawichost zatrudniony na umowę o pracę.
26. **Stażysta, praktykant** - pracownik Urzędu Miasta i Gminy Zawichost odbywający staż lub praktykę na podstawie odrębnie zawartych umów.

2. Osoby odpowiedzialne za bezpieczeństwo informacji i przetwarzanie danych osobowych:

2.1. Obowiązki Administratora Danych:

1) Wdraża odpowiednie środki organizacyjne i techniczne, aby przetwarzanie danych odbywało się zgodnie z prawem, z uwzględnieniem charakteru, kontekstu, zakresu i celu przetwarzania a ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze.
2) Podejmuje decyzje o celach i środkach przetwarzania danych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji i technik zabezpieczania danych,
3) Upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym zakresie, odpowiadającym zakresowi jej obowiązków,
4) Powołuje Inspektora Ochrony Danych (art. 37 RODO).
5) Wyznacza Administratora Systemu Informatycznego (ASI) oraz określa zakres jego zadań i czynności,
6) Prowadzi rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania zgodnie z art. 30 RODO. Administrator Danych może zlecić prowadzenie przedmiotowego rejestru Inspektorowi Ochrony Danych,
7) Dokonuje oceny skutków planowanych operacji przetwarzania danych przed rozpoczęciem ich przetwarzania,
8) Zgłasza naruszenia ochrony danych osobowych do organu nadzorczego oraz zawiadamiania o tym osoby, których te dane dotyczą.

2.2. Powołanie Inspektora Ochrony Danych:

1) Inspektor Ochrony Danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności powinien:
    a) Posiadać fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych osobowych,
    b) Posiadać umiejętność wypełniania zadań określonych w RODO,
    c) Dysponować wiedzą na temat procedur administracyjnych i funkcjonowania jednostki.
2) Administrator Danych po wyznaczeniu Inspektora Ochrony Danych zawiadamia o tym fakcie Prezesa Urzędu Ochrony Danych Osobowych w terminie 14 dni od dnia wyznaczenia.
3) Zmiana danych Inspektora bądź jego odwołanie następuje z zachowaniem terminu 14 dni.
4) Administrator Danych udostępnia na swojej stronie internetowej dane kontaktowe Inspektora tj.: imię nazwisko, nr telefonu lub adres e-mail.

2.3. Rola Inspektora Ochrony Danych:

Inspektor Ochrony Danych pełni funkcję opiniodawczo-doradczo-weryfikacyjną i jest odpowiedzialny w szczególności za:

1) Informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia o Ochronie Danych Osobowych (RODO) oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych osobowych i doradzanie im w tej sprawie,
2) Monitorowanie przestrzegania RODO, innych aktów unijnych lub państw członkowskich, o ochronie danych osobowych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania danych osobowych oraz powiązane z tym audyty,
3) Udzielanie na żądanie zaleceń do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania,
4) Współpracę z organem nadzorczym,
5) Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem,
6) Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z uprzednimi konsultacjami, jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób oraz w stosownych przypadkach prowadzenie konsultacji we wszystkich innych sprawach,
7) Pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy Rozporządzenia o Ochronie Danych Osobowych,
8) Prowadzenie rejestru czynności lub kategorii czynności przetwarzania na polecenie Administratora Danych.

2.4. Obowiązki Administratora Systemu Informatycznego:

1) Administrator Systemów Informatycznych odpowiedzialny jest za zarządzanie i bieżący nadzór nad systemem informatycznym Administratora Danych, w tym:
   a) Przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa lub wyłącza konta użytkowników zgodnie z zapisami niniejszego dokumentu,

b) Resetuje hasła dostępu na poszczególnych stacjach, ujawniając je wyłącznie danemu użytkownikowi,

c) W sytuacji naruszenia zabezpieczeń systemu informatycznego informuje Inspektora Ochrony Danych i współdziała przy usuwaniu skutków naruszenia,

d) Sprawuje nadzór nad wykonywaniem: napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, kopii zabezpieczających, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii sytemu informatycznego,

e) Podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji,

f) Prowadzi nadzór nad ewidencją i inwentaryzuje sprzęt komputerowy i oprogramowanie.

3. Podstawy przetwarzania danych osobowych:

Urząd Miasta i Gminy Zawichost działa wyłącznie w granicach określonych przepisami prawa i przetwarza dane osobowe osób fizycznych wyłącznie w oparciu o przesłanki określone w art. 6 Rozporządzenia 2016/679. Przetwarzanie danych dopuszczalne jest w następujących sytuacjach:

1) Osoba, której dane dotyczą wyraziła zgodę na przetwarzanie jej danych osobowych w jednym lub większej liczbie określonych celów,
2) Przetwarzanie jest niezbędne do wykonania umowy, gdzie stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą przed zawarciem umowy,
3) Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej,
4) Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze,
5) Przetwarzanie jest niezbędne do wykonania zadań realizowanych w interesie publicznym lub do sprawowania władzy publicznej powierzonej Administratorowi.

4. Obowiązek informacyjny:

Administrator Danych podczas pozyskiwania danych od osoby, której dane dotyczą jest zobowiązany poinformować tę osobę o:

1) Swojej tożsamości i danych kontaktowych,
2) Danych kontaktowych Inspektora Ochrony Danych,
3) Celu i podstawie prawnej przetwarzania tych danych osobowych,
4) Odbiorcach danych lub kategorii odbiorców,

5) Okresie, przez który te dane będą przechowywane, a gdy nie jest to możliwe, kryteria ustalenia takiego okresu,
6) Prawie do żądania od Administratora:
    a) dostępu do danych osobowych osoby, której te dane dotyczą,
    b) do sprostowania jej danych osobowych,
    c) do usunięcia jej danych osobowych,
    d) do ograniczenia przetwarzania jej danych osobowych,
    e) do wniesienia sprzeciwu wobec przetwarzania jej danych osobowych,
    f) do przenoszenia danych;
7) Prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem - jeżeli przetwarzanie odbywa się na podstawie zgody,
8) Prawie wniesienia skargi do organu nadzorczego,
9) Właściwości: czy podanie danych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą jest zobowiązana do ich podania i jakie są ewentualne konsekwencje nie podania tych danych,
10) Zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,
11) Zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
12) W przypadku zbierania danych nie od osoby, której dane dotyczą, osobę tę należy poinformować dodatkowo o kategorii i źródle pochodzenia danych osobowych.

5. Prawa osoby, której dane dotyczą:

1) Osoba, której dane dotyczą ma prawo:
    a) Żądania od Administratora dostępu do swoich danych,
    b) Do sprostowania swoich danych,
    c) Do usunięcia swoich danych,
    d) Do ograniczenia przetwarzania swoich danych,
    e) Do wniesienia sprzeciwu do przetwarzania swoich danych

f) Do przenoszenia danych.

2) Każda osoba, której dane dotyczą, ma prawo skorzystać z niniejszych praw poprzez złożenie wniosku do organizacji.
3) Przedmiotowy wniosek zostaje dekretowany do Inspektora Ochrony Danych, który analizuje treść dokumentu, po której sporządza notatkę i w formie pisemnej przedstawia propozycję wykonania czynności Administratorowi Danych wraz z przedmiotowym wnioskiem.
4) Administrator Danych po weryfikacji przedstawionych dokumentów kieruje do Pracownika merytorycznego wniosek i udziela zaleceń dot. odpowiedzi na przedmiotowy dokument, której udziela wskazany przez ADO pracownik.

6. Udostępnianie danych osobowych:

1) Administrator Danych udostępnia przetwarzane dane osobowe tylko osobom lub podmiotom uprawnionym do ich otrzymania na podstawie i w granicach przepisów prawa:
   a) Na wniosek osoby, której dane dotyczą,
   b) Za wyraźną zgodą podmiotu, którego dane dotyczą,
   c) Na wniosek podmiotu uprawnionego do otrzymywania danych osobowych (np.: Policji, Prokuraturze),
   d) Na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych.
2) Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystywać wyłącznie w celu dla którego zostały zebrane.
3) W przypadku wpływu wniosku pochodzącego od osoby, której dane dotyczą w sprawie żądania udzielenia informacji na temat przetwarzania jej danych osobowych, odpowiedź na przedmiotowy wniosek następuje w terminie 30 dni od daty jego otrzymania.

7. Zasady dokonywania anonimizacji danych osobowych publikowanych powszechnie, w tym w Biuletynie Informacji Publicznej oraz na stronach internetowych:

1) Pracownik merytoryczny, sporządzający dokumenty, które mają zostać zamieszczone w Biuletynie Informacji Publicznej i/lub na stronach internetowych zobowiązany jest do wstępnej oceny przedmiotowego dokumentu pod względem dopuszczalności publikacji danych osobowych osób fizycznych, które nie pełnią funkcji publicznych/kierowniczych.
2) Jeżeli wstępna ocena wykaże obecność występowania danych osobowych osób fizycznych pracownik zobowiązany jest do dokonania analizy legalności publikacji danych osobowych w przedmiotowym dokumencie, a następnie anonimizacji zawartych w nim danych osobowych

osób fizycznych tj. imion, nazwisk, adresu, stanu zdrowia, nr PESEL itp. (zgodnie z art.6,9,10 RODO).

3) Pracownik odpowiedzialny za publikację przedmiotowych dokumentów w Biuletynie Informacji Publicznej i/lub na stronach internetowych zobowiązany jest do sprawdzenia poprawności dokonanej anonimizacji danych osobowych w tych dokumentach.

8. Upoważnienie do przetwarzania danych osobowych:

1) Do przetwarzania danych osobowych mogą mieć dostęp wyłącznie osoby posiadające pisemne upoważnienie nadane przez Administratora Danych.
2) Wzór upoważnienia stanowi załącznik nr 2 do Księgi, wniosek o nadanie upoważnienia znajduje się w załączniku nr 13 do Księgi.
3) Administrator Danych zobowiązany jest wydać nowe lub cofnąć upoważnienie w przypadku zmiany stanowiska, zakresu obowiązków pracowniczych, przyjęcia do pracy nowej osoby lub w sytuacji, która wpływa bezpośrednio na rodzaj i zakres przetwarzania danych osobowych.
4) Upoważnienie wydawane jest na czas określony lub nieokreślony.
5) Administrator Danych informuje ustnie Kierownika komórki organizacyjnej o nowo zatrudnionym pracowniku.

9. Ewidencja osób upoważnionych:

Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest przez pracownika kadr, a jej wzór stanowi załącznik nr 3 do Księgi. Dokument ten zawiera w szczególności:

a) Imię i nazwisko osoby upoważnionej,
b) Stanowisko/funkcję,
c) Datę nadania i datę ustania upoważnienia,
d) Zakres upoważnienia (czynności przetwarzania),
e) Identyfikator (jeżeli dane przetwarzane są w systemie informatycznym).

10. Rejestr czynności przetwarzania, rejestr kategorii czynności przetwarzania:

Administrator danych zobowiązany jest do prowadzenia rejestru czynności przetwarzania danych osobowych oraz rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora.

11. Umowy powierzenia przetwarzania danych osobowych:

Zasady wskazane poniżej stosuje się do umów zawieranych z podmiotami trzecimi dotyczącymi powierzenia przetwarzania danych osobowych. W szczególności dostawcy usług informatycznych, szkoleniowych, serwisowych. Umowy te powinny zawierać w szczególności:

1) Przedmiot umowy,
2) Czas trwania,
3) Charakter i cel przetwarzania,
4) Rodzaj danych osobowych,
5) Kategorie osób, których dane dotyczą,
6) Obowiązki i prawa Administratora,
7) Zobowiązanie podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie Administratora Danych,
8) Zobowiązanie podmiotu przetwarzającego, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub aby podlegały odpowiedniemu ustawowemu obowiązkowi zachowania w tajemnicy danych, do których będą miały dostęp na podstawie zawartej umowy,
9) Informacje, że podmiot przetwarzający wdroży wszelkie środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa przed rozpoczęciem przetwarzania,

10) Zobowiązanie podmiotu przetwarzającego do korzystania z usług innego podmiotu przetwarzającego tylko po wyrażeniu pisemnej zgody Administratora Danych, zapewniając, że w przypadku wyrażenia zgody przez niego wybrany podmiot przetwarzający spełnia te kryteria, które zostały zawarte w umowie pomiędzy Administratorem a podmiotem przetwarzającym,
11) Biorąc pod uwagę charakter przetwarzania, podmiot przetwarzający w miarę możliwości pomaga Administratorowi Danych poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw zgodnie z RODO,
12) Uwzględniając charakter przetwarzania oraz dostępne mu informacje, podmiot przetwarzający pomaga Administratorowi Danych wywiązać się z obowiązków określonych w art. 32–36 RODO m.in.: pomoc przy informowaniu organu nadzorczego o naruszeniu ochrony danych,
13) Po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora Danych, podmiot przetwarzający usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych,
14) Udostępnia Administratorowi Danych wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia Administratorowi Danych lub audytorowi upoważnionemu przez Administratora Danych przeprowadzanie audytów, w tym inspekcji i przyczynia się do nich,
15) Kary umowne dla podmiotu, któremu powierzono dane osobowe, za każdorazowe naruszenie postanowień umowy w zakresie przetwarzania danych jak również ponoszenia odpowiedzialności za szkodę wyrządzoną osobom trzecim z tego tytułu,
16) Klauzulę dotyczą wypowiedzenia umowy z zachowaniem terminów wypowiedzenia albo bez zachowania terminów wypowiedzenia, w sytuacji, w której podmiot, któremu powierzono przetwarzanie danych osobowych narusza postanowienia ustawy, przepisów wykonawczych albo umowy w tym zakresie.

12. Domyślna ochrona danych (privacy by default):

Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

13. Incydenty ochrony danych:

W przypadku stwierdzenia naruszenia bezpieczeństwa informacji każdy pracownik ma obowiązek zgłosić ten fakt do Inspektora Ochrony Danych lub Administratora Systemu Informatycznego. Definicję incydentu ochrony danych oraz szczegółowe zasady postępowania w przypadku jego zaistnienia opisano w załączniku 5 do Księgi.

14. Procedura retencji danych:

1) Poprzez retencję danych rozumie się ustalenie celu oraz okresu przechowywania zebranych danych osobowych.
2) Pracownik merytoryczny, który przetwarza dane osobowe zobowiązany jest:
    a) dokonać inwentaryzacji przetwarzanych danych osobowych w konkretnych procesach,
    b) sprawdzić miejsce przechowywania danych,
    c) sprawdzić formę przetwarzania danych,
    d) określić cel, dla którego dane zostały zebrane,
    e) określić czas przechowywania danych poprzez analizę przepisów szczegółowych, z których wynika okres przechowywania danych, a jeżeli taki okres nie jest podany, ustalić kryteria ustalenia okresu.
3) Ustalając okres retencji należy wziąć pod uwagę obecną i przyszłą wartość informacji, koszty, ryzyko i zobowiązania związane z przetwarzanie danych, a także realną możliwość zapewnienia, by dane były aktualne.
4) Po ustaniu okresu przechowywania, dane podlegają usunięciu, gdy:
    a) minął okres ich przydatności,
    b) okaże się, że cel, dla którego dane zostały zebrane został osiągnięty.

BURMISTRZ
mgr Katarzyna Kondziołka

15. Szczegółowe wytyczne organizacyjne zawierające w/w procedury stanowią załączniki do Księgi Polityk i Zasad Ochrony Danych Osobowych w Urzędu Miasta i Gminy Zawichost:

- Zał. nr 1 Oświadczenie o znajomości Księgi Polityk i Zasad oraz zachowaniu poufności.
- Zał. nr 2 Upoważnienie do przetwarzania danych osobowych.
- Zał. nr 3 Ewidencja osób upoważnionych.
- Zał. nr 4 Rejestr czynności przetwarzania.
- Zał. nr.5 Zarządzanie incydentami
- Zał. nr 6 Raport z naruszenia.
- Zał. nr 7 Ocena skutków planowanych operacji.
- Zał. nr 8 Analiza ryzyka.
- Zał. nr 9 Polityka kluczy.
- Zał. nr 10 Bezpieczeństwo fizyczne jednostki.
- Zał. nr 11 Zasady bezpieczeństwa na stanowisku pracy.
- Zał. nr 12 Procedura nadawania i wyrejestrowywania uprawnień.
- Zał. nr 13 Wniosek o nadanie upoważnienia/uprawnień.
- Zał. nr 14 Karta ewidencyjna uprawnień użytkownika.
- Zał. nr 15 Zasady konserwacji i serwisowania sprzętu zawierającego dane osobowe.
- Zał. nr 16 Ogólne procedury użytkowania i zabezpieczeń infrastruktury IT.
- Zał. nr 17 Zasady wykorzystania systemu teleinformatycznego.
- Zał. nr 18 Wzór klauzuli informacyjnej.