

Zarządzenie nr 0120.41.2019
Burmistrza Toszka
z dnia 19 czerwca 2019 r.

w sprawie wprowadzenia dokumentacji ochrony danych osobowych w Urzędzie Miejskim w Toszku

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (tekst jednolity: Dz.U. z 2019 r. poz. 506) oraz przepisów 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 (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L. z 2016r. poz.119.1 oraz Ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. z 2018r. poz. 1000 z późn. zm.) zarządzam, co następuje:

§ 1

W Urzędzie Miejskim w Toszku wprowadza się do stosowania dokumentację ochrony przetwarzania danych osobowych, w skład, której wchodzi:

- 1) POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH – stanowiąca załącznik nr 1 do niniejszego Zarządzenia;
- 2) INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH – stanowiąca załącznik nr 2 do niniejszego Zarządzenia;
- 3) POLITYKA CZYSTEGO BIURKA I CZYSTEGO EKRANU - stanowiąca załącznik nr 3 do niniejszego Zarządzenia;
- 4) PROCEDURA DOSTĘPU DO DANYCH NA ŻĄDANIE OSOBY- stanowiąca załącznik nr 4 do niniejszego Zarządzenia;
- 5) PROCEDURA POSTĘPOWANIA W RAZIE ZAISTNIENIA NARUSZENIA PRZETWARZANIA DANYCH OSOBOWYCH – stanowiąca załącznik nr 5 do niniejszego Zarządzenia;
- 6) PROCEDURA REALIZACJI PRAWA DO OGRANICZENIA PRZETWARZANIA- stanowiąca załącznik nr 6 do niniejszego Zarządzenia;
- 7) PROCEDURA REALIZACJI PRAWA DO PRZENOSZENIA DANYCH - stanowiąca załącznik nr 7 do niniejszego Zarządzenia;
- 8) PROCEDURA REALIZACJI PRAWA DO SPROSTOWANIA DANYCH - stanowiąca załącznik nr 8 do niniejszego Zarządzenia;
- 9) PROCEDURA REALIZACJI PRAWA DO SPRZECIWU- stanowiąca załącznik nr 9 do niniejszego Zarządzenia;
- 10) PROCEDURA REALIZACJI PRAWA DO USUNIĘCIA DANYCH - „PRAWO DO BYCIA ZAPOMNIANYM” – stanowiąca załącznik nr 10 do niniejszego Zarządzenia;
- 11) ZASADY UŻYTKOWANIA URZĄDZEŃ MOBILNYCH – stanowiąca załącznik nr 11 do niniejszego Zarządzenia;
- 12) INSTRUKCJA OBSŁUGI SERWEROWNI – stanowiąca załącznik nr 12 do niniejszego Zarządzenia.

§2

1. Każdy pracownik, zgodnie z wykazem jest obowiązany zapoznać się z treścią dokumentów wymienionych w §1.
2. Zobowiązuje się wszystkich pracowników Urzędu Miejskiego w Toszku oraz strony świadczące usługi na rzecz Urzędu Miejskiego w Toszku do przestrzegania przepisów zawartych w dokumentach, o których mowa w § 1.

§ 3

Dokumentacja ochrony przetwarzania danych osobowych wykazana w §1 stanowi dokumentację wewnętrzną i udostępnianie tych dokumentów podlega ograniczeniu zgodnie z art.5 ust.1 Ustawy z dnia 6 września 2001r. o dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330).

§4

Traci moc Zarządzenie nr 0120.44.2015 Burmistrza Toszka z dnia 28.12.2015 r. w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Miejskim w Toszku.

§5

Wykonanie Zarządzenia powierza się Inspektorowi Danych Osobowych, Administratorowi Systemów Informatycznych.

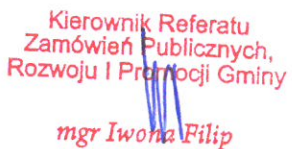
§6

Zarządzenie wchodzi w życie z dniem podpisania.


Zastępca Burmistrza
mgr Piotr Kunce


INFORMATYK
Szymon Kabiza


ADWOKAT
Mateusz Weissensteiner


Kierownik Referatu
Zamówień Publicznych,
Rozwoju i Promocji Gminy
mgr Iwona Filip

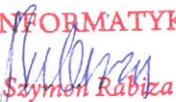
Załącznik nr 1 do zarządzenia Nr 0120.41.2019

Burmistrza Toszka
z dnia 19 czerwca 2019 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

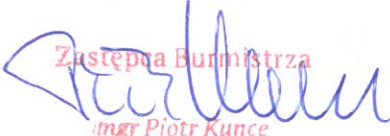
URZĄD MIEJSKI W TOSZKU
UL. BOLESŁAWA CHROBREGO 2
44-180 TOSZEK

INFORMATYK


Szymon Rabiś

Kierownik Referatu
Zamówień Publicznych,
Rozwoju i Promocji Gminy


mgr Iwona Filip

Zastępca Burmistrza

mgr Piotr Kunce

Adwokat


Aleksandra Piotrowska-Wnuk

SPIS TREŚCI

I. POSTANOWIENIA OGÓLNE.....	3
II. PODSTAWOWE POJĘCIA	4
III. BEZPIECZEŃSTWO DANYCH OSOBOWYCH	6
IV. PODSTAWA PRAWNA	7
V. ZAKRES ZASTOSOWANIA	8
VI. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA.....	9
VII. ODPOWIEDZIALNOŚĆ I KOMPETENCJE W ZARZĄDZANIU BEZPIECZEŃSTWEM DANYCH OSOBOWYCH.....	10
VIII. OBOWIĄZEK INFORMACYJNY	13
IX. DOSTĘP DO INFORMACJI.....	14
X. POWIERZANIE DANYCH OSOBOWYCH	15
XI. UDOSTĘPNIANIE DANYCH OSOBOWYCH	16
XII. ANALIZA RYZYKA ZWIĄZANEGO Z PRZETWARZANIEM DANYCH OSOBOWYCH.....	17
XIII.ZABEZPIECZENIE PRZETWARZANYCH DANYCH OSOBOWYCH	19
XIII. ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE	21
XIV. POSTANOWIENIA KOŃCOWE.....	22

I. POSTANOWIENIA OGÓLNE

1. Niniejszy dokument określa zasady bezpieczeństwa przetwarzania danych osobowych jakie powinny być przestrzegane i stosowane w Urzędzie Miejskim w Toszku (zwanym dalej „Urzędem”) przez pracowników i współpracowników, którzy przetwarzają dane osobowe.
2. Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania w Urzędzie informacji zawierających dane osobowe.
3. Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabranie przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO, Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.

II. PODSTAWOWE POJĘCIA

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1. **Administrator danych osobowych (zwany dalej ADO)** oznacza osobę, która ustala cel(e) i sposoby przetwarzania danych osobowych. W omawianym przypadku ADO jest Urząd.
2. **Inspektor Ochrony Danych (zwany dalej IOD)** oznacza osobę, która nadzoruje przestrzeganie zasad ochrony danych osobowych, określonych przez ADO (zgodnie z wytycznymi określonymi w art. 37 RODO).
3. **Administrator Systemu Informatycznego (zwany dalej ASI)** oznacza osobę odpowiedzialną za funkcjonowanie i bezpieczeństwo systemów informatycznych przetwarzających dane osobowe.
4. **Dane osobowe** oznaczają wszelkie informacje dotyczące jednostki, które pozwalają na jej identyfikację niezależnie od stosowanego środka komunikacji (np. papierowego, elektronicznego, video, audio). Przykładami danych osobowych są dane kontaktowe – imię i nazwisko, numer telefonu, numer PESEL, adresy IP, zdjęcia, historia przeglądania stron internetowych, geolokalizacja.
5. **Dane wrażliwe (inaczej szczególne kategorie danych)** oznaczają informacje dotyczące pochodzenia rasowego lub etnicznego; poglądów politycznych; przekonań religijnych lub innych przekonań światopoglądowych; przynależność do związków zawodowych; zdrowia fizycznego lub psychicznego; życia seksualnego; danych genetycznych; danych biometrycznych (np. pobieranie odcisków palców, system rozpoznawania rysów twarzy, skan siatkówki oka); informacje o popełnionych przestępstwach lub domniemanych przestępstwach popełnionych przez osobę, której dane dotyczą.
6. **Prezes Urzędu Ochrony Danych Osobowych (zwany dalej PUODO)** - jest organem do spraw ochrony danych osobowych działający na podstawie art. 34 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
7. **Obszar przetwarzania danych osobowych** – są to wszystkie miejsca w Urzędzie, gdzie dochodzi do przetwarzania danych osobowych. Obszar przetwarzania stanowią także lokalizacje podmiotu przetwarzającego dane, które Urząd powierzył do przetwarzania.

8. **Naruszenie ochrony danych osobowych/naruszenie** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych (np. wiadomość e-mail zostaje nieumyślnie wysłana do nieprawidłowych adresatów, papierowy rejestr zostaje zgubiony lub ukradziony, cyberatak przeprowadzony przez hakerów).
9. **Przetwarzanie** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
10. **Podmiot przetwarzający (procesor)** oznacza podmiot zewnętrzny, który przetwarza dane osobowe w imieniu Urzędu (ADO) w celu zrealizowania przedmiotu umowy. Takimi podmiotami mogą być np. usługodawcy hostingu, BHP, usług serwisowych, firm archiwizujących bądź niszczących dokumenty.
11. **Profilowanie** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych w celu analizy lub prognozy osobowości lub niektórych cech osobowych odnoszących się do jednostki (np. analiza i prognoza zdrowia, sytuacji ekonomicznej, efektów pracy, lokalizacji, przemieszczania się, osobistych preferencji lub zainteresowań, zachowań w sieci takich jak historia przeglądania).
12. **Nośniki danych** – wszelkie nośniki, na których informacje zapisane są w postaci elektronicznej, w szczególności dyski, dyskietki, dyski CD-ROM, karty magnetyczne lub pamięci przenośne.
13. **Zbiór danych osobowych** – każdy posiadający strukturę logiczną zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

III. BEZPIECZEŃSTWO DANYCH OSOBOWYCH

1. Utrzymanie bezpieczeństwa przetwarzanych w Urzędzie informacji, w tym danych osobowych rozumiane jest, jako zapewnienie ich poufności, integralności i rozliczalności na odpowiednim poziomie.
2. Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do danych:
 - 2.1 Poufność danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
 - 2.2 Integralność danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
 - 2.3 Rozliczalność danych – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
3. Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
 - 3.1 Niezaprzeczalności odbioru - rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie.
 - 3.2 Niezaprzeczalności nadania - rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie.
4. Realizując Politykę Bezpieczeństwa w zakresie ochrony danych osobowych Urząd dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
 - 4.1 Przetwarzane zgodnie z prawem.
 - 4.2 Zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnego z tymi celami.
 - 4.3 Merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane.
 - 4.4 Przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej jednak niż jest to niezbędne do osiągnięcia celu przetwarzania.

IV. PODSTAWA PRAWNA

Polityka Bezpieczeństwa Danych Osobowych (zwana w dalszej części „Polityką”) została utworzona w związku z dobrą praktyką prowadzenia przez ADO dokumentacji związanej z ochroną danych osobowych w oparciu o:

1. Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r. poz. 1000 z późn. zm.).
2. Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych - RODO) – art. 24.
3. Ustawę z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. z 2019 r. poz. 506)
4. Ustawę z dnia 21 listopada 2008 r. o pracownikach samorządowych (t.j. Dz.U. z 2018 r. poz. 1260).

INFORMATYK

Szymon Rabiza

V. ZAKRES ZASTOSOWANIA

Zasady określone przez niniejszy dokument mają zastosowanie do całego systemu przetwarzania danych, a w szczególności do:

1. Wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz będących w formie papierowej, w których przetwarzane są lub będą dane osobowe.
2. Informacji będących własnością Urzędu lub jednostek obsługiwanych, o ile zostały przekazane na podstawie umów lub porozumień.
3. Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych, oraz innych dokumentów zawierających dane osobowe.
4. Wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się dane osobowe podlegające ochronie.
5. Wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.
6. Wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

VI. STRUKTURA DOKUMENTÓW POLITYKI BEZPIECZEŃSTWA

1. Dokumenty Polityki Bezpieczeństwa ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Zestaw dokumentów Polityki Bezpieczeństwa składa się z:
 - 2.1. Niniejszego dokumentu Polityki Bezpieczeństwa.
 - 2.2. Instrukcji zarządzania systemami informatycznymi w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych osobowych w Urzędzie.
 - 2.3. Wzoru oświadczenia pracownika do przetwarzania danych osobowych – Załącznik nr 1 Polityki.
 - 2.4. Wzoru upoważnienia dla pracownika do przetwarzania danych osobowych – Załącznik nr 2 Polityki.
 - 2.5. Wzoru ewidencji osób upoważnionych do przetwarzania danych osobowych – Załącznik nr 3 Polityki.
 - 2.6. Wzoru procedury postępowania na wypadek zaistnienia incydentu związanego z przetwarzaniem danych osobowych – Załącznik nr 4 Polityki.
 - 2.7. Wzoru rejestru naruszeń ochrony danych osobowych – Załącznik nr 5 Polityki.
 - 2.8. Wzoru raportu z naruszenia danych osobowych – Załącznik nr 6 Polityki.
 - 2.9. Wzoru rejestru realizacji żądań podmiotu danych – Załącznik nr 7 Polityki.
 - 2.10. Wzoru umowy powierzenia przetwarzania danych osobowych – Załącznik nr 8 Polityki.
 - 2.11. Wzoru analizy ryzyka – Załącznik nr 9 Polityki.
 - 2.12. Wzoru Analizy organizacyjnych środków bezpieczeństwa informacji – Załącznik nr 10 Polityki

VII. ODPOWIEDZIALNOŚĆ I KOMPETENCJE W ZARZĄDZANIU BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

1. Za przetwarzanie danych osobowych niezgodnie z prawem, z powierzonymi celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą, grozi odpowiedzialność karna wynikająca z przepisów RODO, lub pracownicza na zasadach określonych w Kodeksie pracy.
2. Do zadań ADO należy:
 - 2.1. Zapewnienie środków technicznych i organizacyjnych do ochrony przetwarzanych danych osobowych, odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, w szczególności zabezpieczeniem danych przed:
 - Udostępnieniem osobom nieupoważnionym.
 - Zabranieniem przez osobę nieuprawnioną.
 - Zmianą, utratą, uszkodzeniem lub zniszczeniem.
 - 2.2. Zapewnienie legalności przetwarzania danych osobowych, a w szczególności zadbanie, by:
 - Została pozyskana zgoda osoby, której dane dotyczą lub została spełniona inna przesłanka dopuszczająca przetwarzanie danych osobowych.
 - Został spełniony obowiązek informacyjny wobec osoby, której dane dotyczą.
 - Dane były przetwarzane zgodnie z obowiązującymi przepisami prawa oraz normami i dobrymi praktykami oraz normami społecznymi.
 - Dane zbierane były w oznaczonym zgodnym z prawem celem.
 - Dane były merytorycznie poprawne oraz zakres danych był adekwatny do celu zbierania.
 - Były przetwarzane z ograniczeniem czasowym.
 - 2.3. Wyznaczenie Inspektora Ochrony Danych lub w sytuacji, gdy tego nie robi – realizowanie jego zadań zgodnie z art. 24 RODO.
 - 2.4. Dopuszczanie do przetwarzania danych wyłącznie osoby zaznajomionej z przepisami z zakresu ochrony danych osobowych i posiadającej imienne upoważnienie, oraz wydawanie i zarządzanie upoważnieniami.
 - 2.5. Nadzorowanie i dbanie o zgodne z prawem przekazywanie danych osobowych (udostępnianie i powierzanie).
 - 2.6. Respektowanie prawa osób, których dane dotyczą, a w szczególności prawa do uzyskania informacji o:

- ADO.
- Celu, zakresie i sposobie przetwarzania danych.
- Terminu od kiedy i jakie dane są przetwarzane.
- Źródle, z którego dane pochodzą.
- Sposobie udostępniania danych oraz ich odbiorcach.

3. Do zadań IOD należy:

- 3.1. Sporządzanie i wprowadzenie w życie zasad bezpiecznego przetwarzania danych osobowych.
- 3.2. Nadzór nad aktualizacją „Polityki bezpieczeństwa danych osobowych” zawierającej strategię ochrony danych przetwarzanych w systemach informatycznych oraz nadzorowanie przestrzegania określonych w niej zasad.
- 3.3. Nadzór nad aktualizacją wraz z ASI „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych” i czuwanie nad jej przestrzeganiem.
- 3.4. Prowadzenie i aktualizacja ewidencji osób upoważnionych do przetwarzania danych osobowych.
- 3.5. Zarządzanie upoważnieniami do przetwarzania danych osobowych.
- 3.6. Prowadzenie rejestru zbioru danych osobowych.
- 3.7. Nadzorowanie obiegu oraz przechowywania dokumentów zawierających dane osobowe.
- 3.8. Uczestniczenie w czynnościach kontrolnych Organu Nadzoru.
- 3.9. Nadzorowanie fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe, w tym nadzorowanie dostępu do tych pomieszczeń oraz kontrolę przebywających w nich osób.
- 3.10. Nadzorowanie szkoleń personelu z zakresu bezpieczeństwa przetwarzania danych osobowych.
- 3.11. Nadzorowanie bieżących procesów przetwarzania danych, w tym analizę sytuacji oraz przyczyn, które doprowadziły do naruszenia zasad bezpieczeństwa.

4. Do zadań ASI należy:

- 4.1. Przestrzeganie zasad ochrony danych osobowych określonych w „Polityce bezpieczeństwa danych osobowych” oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych” i dokumentach z nimi związanych.

- 4.2. Zapewnienie prawidłowej eksploatacji systemu informatycznego, zgodnej z celami przetwarzania danych osobowych.
 - 4.3. Nadzorowanie wykonywania kopii zapasowych, odpowiedniego ich przechowywania oraz okresowego sprawdzania pod kątem ich dalszej przydatności do odtwarzania danych osobowych w przypadku awarii systemu.
 - 4.4. Zapewnienie ochrony nośników zawierających kopie zbiorów danych osobowych.
 - 4.5. Realizację wytycznych ADO w zakresie ochrony danych osobowych przetwarzanych z wykorzystaniem środków informatycznych.
 - 4.6. Wyjaśnianie wszystkich zgłoszonych nieprawidłowości i incydentów.
5. Do zadań każdego Pracownika i/lub współpracownika Urzędu należy:
- 5.1. Zapoznanie się z zasadami określonymi w niniejszej Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym. Pracownik potwierdza swoją znajomość Polityki przez podpisanie oświadczenia o zapoznaniu się z Polityką.
 - 5.2. Przestrzeganie zasad określonych w niniejszej Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.
 - 5.3. Ochrona prawa do prywatności osób fizycznych powierzających Urzędowi swoje dane osobowe, poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w polityce bezpieczeństwa i Instrukcji Zarządzania Systemem informatycznym Urzędu.

VIII. OBOWIĄZEK INFORMACYJNY

1. W przypadku zbierania danych osobowych na formularzach, umowach, drukach (zarówno papierowych jak i elektronicznych) należy umieszczać na nich odpowiednią klauzulę informacyjną. Klauzula taka powinna informować osobę, której dane zbieramy o:
 - 1.1. Adresie siedziby i pełnej nazwie ADO.
 - 1.2. Celu zbierania danych.
 - 1.3. Prawie dostępu do treści swoich danych oraz ich poprawiania.
 - 1.4. Dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Oraz zgodnie z regulacjami określonymi w RODO:

 - 1.5. Informacji o profilowaniu (bądź nie) przetwarzanych danych osobowych.
 - 1.6. Prawie do przenoszenia przetwarzanych przez ADO danych osobowych.
 - 1.7. Prawie do sprzeciwu, ograniczeniu przetwarzanych danych osobowych.
 - 1.8. Prawie do bycia zapomnianym.
2. Przepisu określonego w ust. 1 nie stosuje się, jeżeli:
 - 2.1. Przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania.
 - 2.2. Osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1
3. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, ADO jest zobowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:
 - 3.1. Adresie siedziby i pełnej nazwie ADO.
 - 3.2. Celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych.
 - 3.3. Źródle danych.
 - 3.4. Prawie dostępu do treści swoich danych oraz ich poprawiania.
 - 3.5. Uprawnieniach wynikających z art. 14 RODO.
4. Przepisu określonego w ust. 1 nie stosuje się w przypadkach określonych w art. 13 pkt 4, oraz art. 14 pkt. 5 a. b. c. d. RODO.

IX. DOSTĘP DO INFORMACJI

1. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Urzędzie zasad ochrony danych osobowych.
2. Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.
3. Udostępnianie danych osobowych podmiotom upoważnionym do ich otrzymania, na podstawie przepisów prawa, powinno odbywać się wg określonych odrębnymi przepisami procedur postępowania.
4. Dostęp do danych osobowych może mieć wyłącznie osoba zaznajomiona z przepisami ustawy o ochronie danych osobowych oraz zasadami zawartymi w obowiązującej w Urzędzie Polityce Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.

X. POWIERZANIE DANYCH OSOBOWYCH

1. ADO może powierzyć przetwarzanie danych osobowych innemu podmiotowi na podstawie umowy powierzenia zawartej na piśmie, z zastrzeżeniem wyjątków wynikających z przepisów powszechnie obowiązującego prawa.
2. Przekazanie zbiorów podmiotowi zewnętrznemu w celu ich przetwarzania nie powoduje zmiany właściwego ADO, którym pozostaje Urząd.
3. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych zobowiązany jest wykorzystywać powierzone mu dane wyłącznie w celach i w zakresie, które zostały wskazane w zawartej z nim umowie.
4. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych obowiązany jest w szczególności do:
 - 4.1. Stosowania odpowiednich środków ochrony danych osobowych, w tym do zapewnienia fizycznej ochrony pomieszczeń w których przetwarzane są dane oraz tworzenia kopii bezpieczeństwa systemów informatycznych, w których przetwarzane są powierzone dane osobowe.
 - 4.2. Opracowania dokumentacji dotyczącej przetwarzania danych osobowych.
 - 4.3. Niezwłocznego powiadomienia Urzędu o przypadkach naruszenia przetwarzania powierzonych danych osobowych oraz do dokumentowania wszelkich informacji, które mogą pomóc w ustaleniu okoliczności tego naruszenia, wraz z zachowaniem określonego w Art. 33 RODO terminu na realizację tego powiadomienia.
 - 4.4. Zapewnienia, aby każda osoba stanowiąca personel podmiotu zewnętrznego przetwarzająca powierzone dane osobowe posiadała upoważnienie do przetwarzania tych danych osobowych.
 - 4.5. Zniszczenia lub zwrotu przekazanych danych stosownie do zapisów umowy powierzenia przetwarzania danych.

XI. UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. Udostępnianie danych osobowych odbiorcom danych może nastąpić, podobnie jak przetwarzanie danych, w przypadku spełnienia jednej z przesłanek określonych w Art. 6 pkt. RODO, tj:
 - 1.1. Osoba, której dane dotyczą, wyrazi na to zgodę.
 - 1.2. Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.
 - 1.3. Jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.
 - 1.4. Jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.
 - 1.5. Jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.
2. Osoby upoważnione do przetwarzania danych, którzy w ramach swych obowiązków służbowych udostępniają dane osobowe mają obowiązek prowadzić ewidencję danych, które są udostępniane (określającą odbiorcę danych, przyczynę udostępnienia, zakres danych oraz datę udostępnienia).

XII. ANALIZA RYZYKA ZWIĄZANEGO Z PRZETWARZANIEM DANYCH OSOBOWYCH

1. Identyfikacja zagrożeń.

FORMA PRZETWARZANIA DANYCH	ZAGROŻENIA
Dane przetwarzane w sposób tradycyjny (papierowe)	• Oszustwo. • Kradzież. • Sabotaż. • Zdarzenia losowe (powódź, pożar, zawalenie budynku itd). • Zaniedbania pracowników (niedyskrecja, przypadkowe/celowe udostępnienie danych osobie nieupoważnionej). • Niekontrolowana obecność osób nieupoważnionych w obszarze przetwarzania danych; pokonanie zabezpieczeń fizycznych. • Podśluchy, podglądy; atak terrorystyczny. • Brak rejestrowania udostępniania danych. • Niewłaściwe miejsce i sposób przechowywania dokumentacji.
Dane przetwarzane w systemach informatycznych	• Wadliwe zarządzanie systemem identyfikatorów. • Niewłaściwa administracja systemem. • Niewłaściwa konfiguracja systemu. • Zniszczenie (sfalszowanie) kont użytkowników. • Kradzież danych kont. • Pokonanie zabezpieczeń programowych. • Zaniedbanie pracowników (niedyskrecja, udostępnianie danych osobom nieupoważnionym). • Niekontrolowana obecność nieuprawnionych osób. • Zdarzenia losowe (powódź, pożar).

	• Niekontrolowane wytwarzanie i wypływ danych poza obszar przetwarzania za pomocą nośników informacji i komputerów przenośnych. • Naprawy i konserwacja systemu lub sieci teleinformatycznej wykonane przez osoby nieuprawnione; przypadkowe lub celowe uszkodzenie systemów i aplikacji informatycznych lub sieci. • Przypadkowe lub celowe wprowadzanie zmian do chronionych danych osobowych; brak rejestrowania zdarzeń, tworzenia lub modyfikowania danych.
--	--

2. Poziom ryzyka naruszenia bezpieczeństwa danych jest niski. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych.
3. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla systemów informatycznych stosuje się wysoki poziom bezpieczeństwa. Okresowo należy przeprowadzić analizę ryzyka dla poszczególnych systemów i na tej podstawie określa środki techniczne i organizacyjne, celem zapewnienia właściwej ochrony przetwarzanym danym.

XIII. ZABEZPIECZENIE PRZETWARZANYCH DANYCH OSOBOWYCH

W Urzędzie należy stosować następujące kategorie środków zabezpieczeń danych osobowych:

1. Zabezpieczenia fizyczne:
 - 1.1. Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane na klucz nie mogą pozostawać otwarte bez opieki właściwego personelu.
 - 1.2. Pomieszczenia, w których przetwarzane są dane osobowe zlokalizowane w miejscach zabezpieczonych przed ingerencją osób nieupoważnionych.
2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
 - 2.1. Przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach.
 - 2.2. Przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby, osoby nieupoważnione nie mogą mieć bezpośredniego dostępu do tych pomieszczeń.
3. Zabezpieczenia organizacyjne:
 - 3.1. Osoby bezpośrednio odpowiedzialne za bezpieczeństwo danych na bieżąco kontrolują z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami, pracę pracowników odpowiedzialnych za przetwarzanie danych osobowych oraz systemu informatycznego.
 - 3.2. Winny być regularnie prowadzone przez ADO kontrole stanu bezpieczeństwa systemów informatycznych i przestrzegania zasad ochrony informacji.
4. Zabezpieczenia informatyczne.
 - 4.1. Zasady bezpiecznego użytkowania systemu informatycznego zawarte są w Instrukcji Zarządzania Systemem Informatycznym, obligatoryjnej do zapoznania się i stosowania przez wszystkich użytkowników systemu informatycznego Urzędu.
 - 4.2. Ochronę danych osobowych należy realizować z wykorzystaniem następujących minimalnych zabezpieczeń:
 - 4.2.1. Przyznawania indywidualnych identyfikatorów.
 - 4.2.2. Zapewnienie stopniowania uprawnień.
 - 4.2.3. Odnotowania daty pierwszego wprowadzenia danych w systemie.
 - 4.2.4. Odnotowania identyfikatora użytkownika wprowadzającego dane.
 - 4.2.5. Odnotowania źródła danych, w przypadku zbierania danych nie od osoby, której dane dotyczą.

- 4.2.6. Odnotowania informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie tego udostępnienia.
 - 4.2.7. Zapewnienie możliwości sporządzenia i wydrukowania raportu zawierającego dane osobowe wraz z informacjami o historii przetwarzania danych.
5. W ramach zabezpieczenia danych osobowych ochronie podlegają:
- 5.1. Sprzęt komputerowy - serwer, komputery osobiste, drukarki i inne urządzenia zewnętrzne.
 - 5.2. Oprogramowanie - kody źródłowe, programy użytkowe, systemy operacyjne, narzędzia wspomagające i programy komunikacyjne.
 - 5.3. Dane zapisane na dyskach oraz dane podlegające przetwarzaniu w systemie.
 - 5.4. Hasła użytkowników.
 - 5.5. Pliki dziennych operacji systemowych i baz danych, kopie zapasowe i archiwa.
 - 5.6. Dokumentacja - zawierająca dane systemu, opisująca jego zastosowanie, przetwarzane informacje.
 - 5.7. Związana z przetwarzaniem danych osobowych dokumentacja papierowa, z której dane są wprowadzane do systemu informatycznego lub też funkcjonują niezależnie od niego.

XIII. ARCHIWIZOWANIE INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE

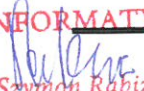
1. Archiwizację dokumentów zawierających dane osobowe prowadzi się w odpowiednio zabezpieczonych pomieszczeniach i na właściwie zabezpieczonych nośnikach informatycznych lub tradycyjnych.
2. Dane zbędne dla prowadzonych spraw są natychmiast niszczone poprzez działania fizyczne i informatyczne uniemożliwiające ich odczytanie.

XIV. POSTANOWIENIA KOŃCOWE

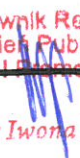
1. Wszyscy pracownicy i współpracownicy Urzędu przetwarzający dane osobowe są zobowiązani do zapoznania się z treścią niniejszej polityki.
2. Polityka bezpieczeństwa wchodzi w życie z dniem podpisania.
3. Jakiegolwiek zmiany wprowadzane w załącznikach do niniejszej polityki nie wymagają zmiany polityki.


Zastępca Burmistrza
mgr Piotr Kunce

INFORMATYK


Szymon Rabiza

Kierownik Referatu
Zamówień Publicznych,
Rozwoju i Promocji Gminy


mgr Iwona Filip

Adwokat

Aleksandra Piotrowska-Wnuk

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

OŚWIADCZENIE PRACOWNIKA PRZETWARZAJĄCEGO DANE OSOBOWE - WZÓR

.....
(nazwisko i imię Pracownika)

.....
(stanowisko)

OŚWIADCZENIE – ochrona danych osobowych

Ja, niżej podpisana/y oświadczam, że do pracy przy przetwarzaniu danych osobowych zostałam/em zaznajomiona/ny z przepisami dotyczącymi ochrony danych osobowych, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO) oraz Ustawą o ochronie danych osobowych z dn. 10 maja 2018 r. (Dz. U. 2018 poz. 1000 z późn. zm.),
a także z Polityką bezpieczeństwa danych osobowych obowiązującą w Urzędzie Miejskim w Toszku.

Jednocześnie zobowiązuję się do postępowania zgodnie z prawem oraz zachowania w poufności danych osobowych, które przetwarzam w trakcie wykonywania obowiązków służbowych.
Zostałam/em poinformowany o odpowiedzialności związanej z przetwarzaniem danych osobowych.

.....
(data i podpis oświadczającego)

UPOWAŻNIENIE Nr...

DO PRZETWARZANIA DANYCH OSOBOWYCH - WZÓR

Toszek, dnia _____

Urząd Miejski, z siedzibą w Toszku przy ulicy Bolesława Chrobrego 2 (zwany w dalszej części upoważnienia „Urzędem”), będące zgodnie z przepisami prawa Administratorem Danych Osobowych

upoważnia Panią/Pana* _____ ⁽¹⁾

do przetwarzania danych osobowych obejmujących następujące procesy przetwarzania:
_____ ⁽²⁾

w następującym zakresie czynności, tj. do prowadzenia operacji na tych danych, takich jak ⁽³⁾:

- ☐ Zbieranie;
- ☐ Utrwalanie;
- ☐ Przechowywanie;
- ☐ Opracowywanie;
- ☐ Zmienianie;
- ☐ Udostępnianie;
- ☐ Przeglądanie;
- ☐ Usuwanie;
- ☐ Inne (proszę określić): _____

1. Upoważnienie udzielane jest wyłącznie w zakresie wynikającym z zadań służbowych pracownika oraz poleceń służbowych. Upoważnienie obejmuje uprawnienie do przetwarzania danych osobowych gromadzonych i przetwarzanych przez Urząd w formie papierowej jak i elektronicznej.
2. Upoważniony jest zobowiązany do zachowania poufności danych.
3. Upoważnienie traci ważność z chwilą jego pisemnego cofnięcia lub ustania stosunku umownego wiążącego upoważnionego z administratorem danych. Wygaśnięcie upoważnienia nie zwalnia z zachowania przez upoważnionego poufności informacji.

(podpis i data Administratora Danych Osobowych)

¹ – należy określić osobę upoważnioną przez podanie imienia i nazwiska;

² – należy określić procesy, w których upoważniony będzie przetwarzał dane osobowe;

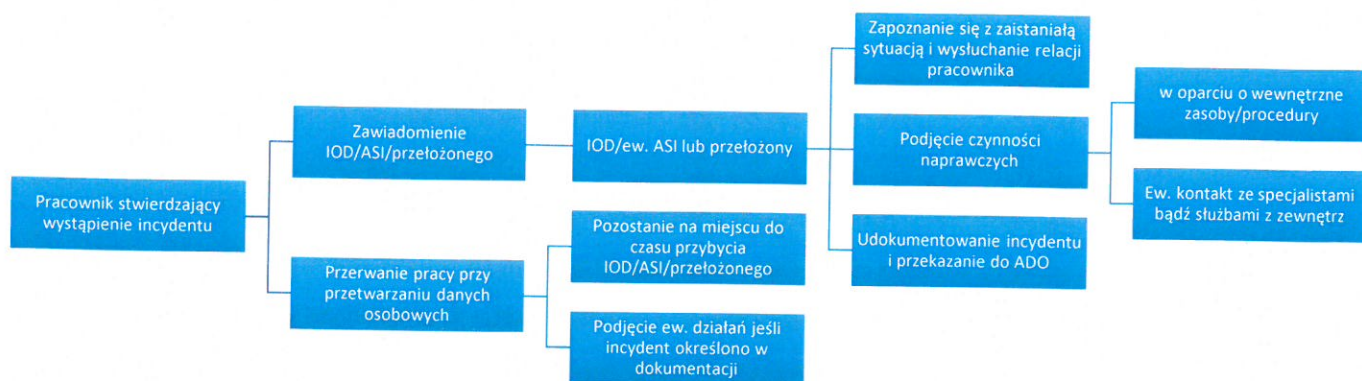
³ – należy zaznaczyć właściwe.

Załącznik nr 3 do Polityki bezpieczeństwa danych osobowych Urząd Miejski w Toszku

EWIDENCJA OSÓB UPOWAŻNIIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH - WZÓR

Imię i nazwisko osoby upoważnionej	Stanowisko służbowe	Zakres upoważnienia do przetwarzania danych osobowych	Nr upoważnienia	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator (jeśli dane przetwarzane są w systemie informatycznym)

Załącznik nr 4 do Polityki bezpieczeństwa danych osobowych Urząd Miejski w Toszku



- 3.7. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu IOD bądź inna osoba upoważniona zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
- 3.8. IOD bądź inna osoba uprawniona po zaistniałym naruszeniu w przetwarzaniu danych osobowych sporządza Raport z naruszenia celem przedstawienia go Administratorowi Danych Osobowych oraz w celach dokumentacyjnych. Wzór wspomnianego Raportu stanowi Załącznik nr 6 Polityki Bezpieczeństwa.
4. Najczęstsze przypadki incydentów związanych z przetwarzaniem danych osobowych:
- 4.1. Naruszenie zabezpieczeń systemu informatycznego bądź oprogramowania przetwarzającego dane osobowe.
- 4.2. Naruszenie technicznego stanu urządzeń służących do przetwarzania danych osobowych.
- 4.3. Naruszenie zawartości zbioru danych osobowych.
- 4.4. Ujawnienie metody pracy lub sposobu działania programu osobie nieupoważnionej do przetwarzania danych osobowych.
- 4.5. Kradzież danych osobowych (zapisanych na nośniku, komputerze, dokumentach papierowych).
- 4.6. Zagubienie bądź wyrzucenie danych osobowych, które pracownik przetwarzał.
- 4.7. Omyłkowe ujawnienie danych osobowych osobie nieupoważnionej (np. poprzez wysyłkę pocztą elektroniczną danych osobowych do niewłaściwego adresata).
- 4.8. Inne zdarzenia mogące mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.).

A. Schemat postępowania w razie naruszenia bezpieczeństwa przetwarzania danych

- 3.3.2. Rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia.
- 3.3.3. Zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę.
- 3.3.4. Podjąć odpowiednie działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej.
- 3.3.5. Nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IOD lub osoby upoważnionej.
- 3.4. Po przybyciu na miejsce zdarzenia, IOD lub inna osoba upoważniona:
 - 3.4.1. Zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Urzędu.
 - 3.4.2. Może żądać dokładnej relacji z zaistniałego incydentu od osoby powiadamiającej.
 - 3.4.3. Może również zażądać relacji od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.
 - 3.4.4. Rozważa celowość i potrzebę powiadomienia o zaistniałym naruszeniu ADO.
 - 3.4.5. Jeśli zachodzi taka konieczność nawiązuje bezpośredni kontakt ze specjalistami spoza Urzędu.
- 3.5. IOD (lub inna osoba uprawniona) dokumentuje zaistniały przypadek naruszenia w rejestrze naruszeń wg wzoru stanowiącego Załącznik nr 5 Polityki Bezpieczeństwa, który zawiera:
 - 3.5.1. Określenie czasu i miejsca naruszenia.
 - 3.5.2. Określenie okoliczności towarzyszących i rodzaju naruszenia.
 - 3.5.3. Skutki naruszenia.
 - 3.5.4. Opis przeprowadzonego postępowania wyjaśniającego i naprawczego.
 - 3.5.5. Określenie czy naruszenie podlega obowiązkowi powiadomienia do Organu Nadzoru.
- 3.6. Jeśli naruszenie i jego ewentualne skutki wymagają zgłoszenia tego faktu do Organu Nadzoru, IOD jest zobowiązany do powiadomienia na drodze pisemnej Organ Nadzoru w ciągu 72 godzin od stwierdzenia naruszenia.

PROCEDURA POSTĘPOWANIA W RAZIE ZAISTNIENIA INCYDENTU
PRZETWARZANIA DANYCH OSOBOWYCH

1. Incydem naruszającym bezpieczeństwo przetwarzania danych osobowych jest każde pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem przetwarzanych danych osobowych, które stwarzają znaczne prawdopodobieństwo zakłócenia prawidłowego przetwarzania danych.
2. Incydenty przetwarzania danych osobowych mogą dotyczyć następujących obszarów:
 - 2.1. Zabezpieczenia systemu informatycznego.
 - 2.2. Technicznego stanu urządzeń.
 - 2.3. Zawartości zbioru danych osobowych.
 - 2.4. Ujawnienia metody pracy lub sposobu działania programu.
 - 2.5. Jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych.
 - 2.6. Innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.).
3. W przypadku podejrzenia lub stwierdzenia naruszenia ochrony danych osobowych ma zastosowanie następująca procedura:
 - 3.1. Każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym fakcie Inspektora Ochrony Danych (IOD) lub inną osobę mogąca podjąć decyzję dotyczącą realizacji dalszych kroków (np. Administratora Systemów Informatycznych - ASI).
 - 3.2. W razie niemożliwości zawiadomienia IOD lub innej osoby określonej w p. 3.1, należy powiadomić bezpośredniego przełożonego,
 - 3.3. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych IOD lub innej upoważnionej osoby (ASI, bezpośredni przełożony), należy:
 - 3.3.1. Niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców.

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH -WZÓR

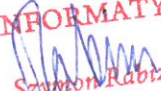
Rodzaj naruszenia	Obowiązek zgłoszenia organowi nadzorczemu	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze

RAPORT Z NARUSZENIA OCHRONY DANYCH - WZÓR

1. Data i godzina wystąpienia naruszenia
.....
.....
2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe):
.....
.....
3. Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):
.....
.....
4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:
.....
.....
5. Podjęte działania:
.....
.....
6. Wstępna ocena przyczyn wystąpienia naruszenia:
.....
.....
7. Postępowanie wyjaśniające i naprawcze:
.....
.....

.....
(data i podpis osoby opracowującej raport)

.....
(data i podpis ADO)

INFORMATYK

Szymon Rabcza

WZÓR REJESTRU REALIZACJI ŻĄDAŃ PODMIOTU DANYCH

I. Żądanie

1. Data zgłoszenia żądania:

.....

2. Forma zgłoszenia żądania (kanał komunikacji):

.....

3. Zgłaszający żądanie:

.....

4. Treść żądania:

.....

II. Obsługa żądania

1. Pracownik obsługujący żądanie:

.....

2. Czy dane zgłaszającego żądanie są przetwarzane przez administratora danych:

.....

3. Czy dane zgłaszającego żądanie zostały powierzone (komu, kiedy):

.....

4. Podjęte czynności:

a) Czynność I

- Osoba podejmująca czynność:

.....

- Opis czynności:

.....

- Data dokonania czynności:

.....

b) Czynność II

- Osoba podejmująca czynność:

.....

- Opis czynności:

.....

- Data dokonania czynności:

.....

Umowa powierzenia przetwarzania danych osobowych

Zawarta dnia _____ pomiędzy:

_____ (*dane podmiotu który umowę zawiera)

zwany w dalszej części umowy „Podmiotem przetwarzającym”
reprezentowana przez:

_____ oraz

_____ (*dane podmiotu który umowę zawiera)
zwany w dalszej części umowy „Administratorem danych” lub „Administratorem”
reprezentowana przez:

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem”) dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§ 2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane (*należy podać rodzaj danych) np. dane zwykłe (*należy podać kategorię osób, których dane dotyczą) np. pracowników administratora, klientów administratora itd. w postaci np. imion i nazwisk, adresu zamieszkania, nr PESEL itd.
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu (*należy podać cel przetwarzania danych przez podmiot przetwarzający) np. realizacji umowy z dnia nr w zakresie (z umowy o współpracy).

§ 3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków

technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.

2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe (*należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane*) oraz usuwa wszelkie ich istniejące kopie chyba, że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu (**można wskazać np. w ciągu 24 h*).

§4 Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum (**należy wpisać z ilu dniowym wyprzedzeniem Administrator informuje o kontroli*) jego uprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni (**administrator termin może określić dowolnie*).
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5 Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.

2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych, 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 danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §3 ust. 2 Umowy winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiegokolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony** od do
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem * okresu wypowiedzenia.

§8

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:

- a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
- b) przetwarza dane osobowe w sposób niezgodny z umową;
- c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

§9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy chyba, że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych (**lub Podmiotu przetwarzającego w zależności od postanowień stron*).

Administrator danych

Podmiot przetwarzający

Firma:	Urząd Miejski w Toszku
Komórka organizacyjna:	
Imię i nazwisko wypełniającego ankietę:	
Stanowisko wypełniającego ankietę:	

Zagrożenie	Zagrożone aktywa	Prawdopodobieństwo				Wpływ na aktywa				P	I	Ryzyko	Podjęte działania
		Wystąpienie zdarzenia	Ekspozycja	Czas	Poufność	Integralność	Dostępność						
1	2	3	4	5	6	7	8	9	10	11	12		
Zażalenie		0	0	0	0	0	0	0	0	0			
Powódź		0	0	0	0	0	0	0	0	0			
Pożar (wewnątrz budynku)		0	0	0	0	0	0	0	0	0			
Pożar (na zewnątrz budynku)		0	0	0	0	0	0	0	0	0			
Blockada dróg i dostaw spowodowana pogodą (wichura, śnieżycą)		0	0	0	0	0	0	0	0	0			
Zagrożenie terrorystyczne		0	0	0	0	0	0	0	0	0			
Epidemia		0	0	0	0	0	0	0	0	0			
Wybuch gazu/paliw		0	0	0	0	0	0	0	0	0			
Katastrofa budowlana		0	0	0	0	0	0	0	0	0			
Brak dostawy prądu		0	0	0	0	0	0	0	0	0			
Brak dostawy wody		0	0	0	0	0	0	0	0	0			
Brak dostawy paliw		0	0	0	0	0	0	0	0	0			
Brak dostępu do Internetu		0	0	0	0	0	0	0	0	0			
Awaria klimatyzacji		0	0	0	0	0	0	0	0	0			
Awaria systemu poz		0	0	0	0	0	0	0	0	0			
Sabotaż wewnętrzny		0	0	0	0	0	0	0	0	0			
Kradzież dokumentów przez osoby upoważnione		0	0	0	0	0	0	0	0	0			
Kradzież dokumentów przez osoby nieupoważnione		0	0	0	0	0	0	0	0	0			
Odeście pracownika do konkurencji		0	0	0	0	0	0	0	0	0			
Kradzież dokumentów przez osoby z zewnątrz		0	0	0	0	0	0	0	0	0			
Kradzież z włamaniem		0	0	0	0	0	0	0	0	0			
Atak hakerski		0	0	0	0	0	0	0	0	0			
Błąd administratora		0	0	0	0	0	0	0	0	0			
Błąd dostawcy usług zewnętrznych		0	0	0	0	0	0	0	0	0			
Awaria nośników danych		0	0	0	0	0	0	0	0	0			
Brak backupu danych		0	0	0	0	0	0	0	0	0			
Niepowodzenie w odzyskaniu danych z backupu		0	0	0	0	0	0	0	0	0			
Przerwa w dostarczaniu usługi kluczowej z punktu widzenia biznesu		0	0	0	0	0	0	0	0	0			
Awaria u dostawcy usług zewnętrznych (poczta, hosting itd.)		0	0	0	0	0	0	0	0	0			
Negatywne efekty działań urzędu skarbowego lub innych instytucji		0	0	0	0	0	0	0	0	0			
Bankructwo zewnętrznego dostawcy usług lub towarów		0	0	0	0	0	0	0	0	0			
Kara umowna		0	0	0	0	0	0	0	0	0			
Błąd księgowy		0	0	0	0	0	0	0	0	0			
Niedyspozycyjność osób kluczowych dla działalności		0	0	0	0	0	0	0	0	0			
Kradzież telefonu komórkowego		0	0	0	0	0	0	0	0	0			
Kradzież kart bankowych, np. kredytowych/debetowych		0	0	0	0	0	0	0	0	0			
Brak dostarczenia zamówionego towaru		0	0	0	0	0	0	0	0	0			
Opóźnienie w dostarczaniu zamówionego towaru		0	0	0	0	0	0	0	0	0			
Awaria sprzętu sieciowego		0	0	0	0	0	0	0	0	0			
Awaria serwerów		0	0	0	0	0	0	0	0	0			
Awaria oprogramowania		0	0	0	0	0	0	0	0	0			
Kradzież laptopa		0	0	0	0	0	0	0	0	0			
Infekcja złośliwym oprogramowaniem		0	0	0	0	0	0	0	0	0			
Atak socjotechniczny (phishing, telefon)		0	0	0	0	0	0	0	0	0			
Brak reakcji administratora		0	0	0	0	0	0	0	0	0			
Wysycenie zasobów		0	0	0	0	0	0	0	0	0			

Analiza organizacyjnych środków bezpieczeństwa informacji

Lp.	Zagadnienia / Obowiązujące wymagania / Zakres kontroli	Rekomendacje / Zalecenia	Stan faktyczny / Uwagi / Zalecane rozwiązania	Data, imię, nazwisko lub stanowisko osoby kontrolującej lub odpowiedzialnej
1.	Analiza i aktualizacja Polityki bezpieczeństwa służącej do przetwarzania danych osobowych. Dostosowanie do RODO.	Przegląd oraz aktualizacja dokumentacji powinien odbywać się nie rzadziej niż raz na rok.		
2.	Analiza i aktualizacja Instrukcji zarządzania systemem informatycznym służącej do przetwarzania danych osobowych. Dostosowanie do RODO.	Przegląd oraz aktualizacja dokumentacji powinien odbywać się nie rzadziej niż raz na rok.		
3.	Analiza praw i obowiązków administratora systemu informatycznego (ASI). Sposób formalnego wyznaczenia.	Pisemne określenie szczegółowego zakresu czynności, obowiązków, uprawnień administratora systemów informatycznych.		

Załącznik nr 10 do Polityki bezpieczeństwa danych osobowych Urząd Miejski w Toszku

4.	Przeprowadzenie inwentaryzacji aktywów w zakresie informacji, które mają wartość dla administratora danych.	Wskazanie grupy informacji podlegających ochronie włączając w to dane osobowe pracowników ADO.	
5.	Sprawdzenie zakresu, rodzaju zbieranych danych, celów, w jakich są zbierane i adekwatności.	Sprawdzenie zasady celowości, adekwatności, merytorycznej poprawności oraz ograniczenia czasowego.	
6.	Podjęmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji mają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, które mają na celu zapewnienie bezpieczeństwa informacji.	Sprawdzenie sposobu nadawania upoważnień do przetwarzania danych oraz ich zakresu. Sprawdzenie aktualności i sposobu prowadzenia ewidencji osób upoważnionych do przetwarzania danych. Zebranie oświadczeń o zachowaniu tajemnicy służbowej	

Załącznik nr 10 do Polityki bezpieczeństwa danych osobowych Urząd Miejski w Toszku

		przetwarzaniu danych zgodnie z obowiązującymi przepisami.		
7.	Sprawdzenie treści klauzul informacyjnych i klauzul zgody na przetwarzanie danych.	Określenie sposobu realizacji obowiązku informacyjnego.		
8.	Zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.	Sprawdzenie umów z zewnętrznymi firmami pod kątem możliwości powierzenia lub dostępu do danych. Zawarcie umowy powierzenia. Prowadzenie ewidencji podmiotów zewnętrznych.		
9.	Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.	Zarządzanie ryzykiem. Stworzenie mapy ryzyk. Określenie zadań i celów.		

10.	Zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji.	Przeprowadzanie szkoleń stanowiskowych. Opracowanie kart szkoleniowych. Zebranie oświadczeń pracowników. Jeżeli zajdzie taka potrzeba to prowadzenie szkoleń z udziałem zewnętrznych specjalistów.		
11.	Opis i zabezpieczenie obszaru przetwarzania danych.	Przygotowanie wykazu pomieszczeń, w których przetwarzane są dane osobowe. Odpowiednie gospodarowanie kluczami. Stosowanie fizycznych środków bezpieczeństwa (ochrona fizyczna, kraty, alarmy, monitoring itp.).		

Załącznik nr 10 do Polityki bezpieczeństwa danych osobowych Urząd Miejski w Toszku

12.	Określenie sposobów zabezpieczenia danych przetwarzanych w formie papierowej.	Stosowanie zasady „czystego biurka”. Stosowanie zamkniętych metalowych i niemetalowych szaf. Określenie sposobów przechowywania kluczy w szafach. Stosowanie niszczarek dokumentów.		
13.	Zabezpieczenia przed skutkami pożaru.	Stosowanie systemów gaszenia pożaru lub wolnostojących, odpowiednich gaśnic. Przygotowanie planów ewakuacji, wyznaczenie miejsc zbiórki dla ludzi i sprzętu.		

		Przechowywanie kopii bezpieczeństwa w innej lokalizacji.		
14.	Obieg i archiwizacja dokumentów.	Prowadzenie rejestru korespondencji. Przygotowanie instrukcji obiegu dokumentów. Przygotowanie instrukcji archiwalnej wraz z zasadami brakowania dokumentów. Przygotowanie instrukcji kancelaryjnej.		
15.	Określenie sposobu publikowania i udostępniania informacji publicznych. Realizacja ustawy o dostępie do informacji publicznej.	Prowadzenie Biuletynu Informacji Publicznej. Realizacja wniosków o udostępnienie informacji publicznej. Prowadzenie strony WWW.		

Analiza technicznych i informatycznych środków bezpieczeństwa informacji

16.	Tryb i częstotliwość tworzenia kopii zapasowych.	Procedury wykonywania i odtwarzania kopii zapasowych. Przechowywanie kopii w innej lokalizacji. Testowanie kopii – protokoły z testowania.		
17.	Plany ciągłości działania systemów informatycznych w przypadku wystąpienia awarii katastrofalnej.	Plan odbudowy oprogramowania po awarii. Plan utrzymania ciągłości działania systemów informatycznych.		
18.	Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.	Raport z inwentaryzacji komputera. Raport podsumowujący inwentaryzację oprogramowania. Rejestr komputerów przenośnych.		

19.	Dziennik administratora systemu informatycznego. Rejestr incydentów.	Dokumentowanie czynności z zakresu eksploatacji, aktualizacji i monitoringu systemu i oprogramowania. Raporty z naruszenia ochrony danych. Rejestr incydentów bezpieczeństwa i działań korygujących i zapobiegawczych.		
20.	Proces uwierzytelniania i identyfikacji użytkowników w systemie.	Konta użytkowników i loginy. Polityka haseł. Identyfikacja osób dokonujących wpisu.		
21.	Rozliczalność w systemach teleinformatycznych.	Historia logów.		
22.	Bezzwłoczna zmiana uprawnień w przypadku zmiany zadań osób upoważnionych lub ustania upoważnienia.	Blokowanie haseł i kont byłego pracownika. Zwrot sprzętu i innych aktywów.		

Załącznik nr 10 do Polityki bezpieczeństwa danych osobowych Urząd Miejski w Toszku

23.	Czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji.	Badanie podatności i wykrywanie słabych punktów systemu i stron WWW. Aktualizacja oprogramowania, w tym antywirusowego.		
24.	Środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.	Legalność i aktualność programu antywirusowego. Firewall do ochrony dostępu do sieci komputerowej. System IDS/IPS (systemy wykrywania i zapobiegania awariom)		
25.	Zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.	Ewidencja laptopów. Hasła na BIOS lub programy szyfrujące. Szyfrowane połączenia i protokoły.		
26.	Minimalizowanie ryzyka utraty informacji w wyniku awarii.	UPS, generator prądu itp.		

		Listwy przepięciowe. Kopie zapasowe.		
27.	Ochrona przed błędami, utratą, nieuprawnioną modyfikacją.	Integralność danych i systemów jako brak możliwości nieuprawnionych zmian, kopiowania, usuwania.		
28.	Stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa.	Szyfrowany protokół SSL (<i>bezpieczna wymiana danych za pomocą Internetu</i>) VPN. Bezpieczeństwo sieci.		
29.	Mechanizmy automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.	Wygaszacze ekranów zabezpieczone hasłem. Blokowanie stanowiska pracy.		

Załącznik nr 10 do Polityki bezpieczeństwa danych osobowych Urząd Miejski w Toszku

30.	Zasady bezpiecznego korzystania z Internetu i poczty elektronicznej.	Blokowanie zbędnych i groźnych stron i treści. Monitoring sieci i poczty.		
31.	Zabezpieczenie serwerowni.	Wydzielenie pomieszczenia. System kontroli dostępu. Klimatyzacja lub pomiar temperatury i wilgotności.		
32.	Bezpieczeństwo krytycznych urządzeń sieciowych.	Zdublowane switchy, routery. Wydzielona sieć energetyczna.		
33.	Bezpieczeństwo danych na dyskach i innych nośnikach informacji przeznaczonych do naprawy lub likwidacji.	Pozbawianie lub uszkadzanie zapisu danych. Nadzór osób upoważnionych. Umowy powierzenia. Protokoły i raporty usuwania danych.		

Załącznik nr 10 do Polityki bezpieczeństwa danych osobowych Urząd Miejski w Toszku

34.	Bezpieczeństwo i zasady współpracy z podmiotami zewnętrznymi, np. dostawcami lub serwisantami oprogramowania czy serwerów.	Zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji. Zawieranie umów powierzenia przetwarzania danych osobowych w przypadku stałej współpracy.	
-----	---	---	--

Załącznik nr 2 do zarządzenia Nr 0120.41.2019

Burmistrza Toszka
z dnia 19 czerwca 2019 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

URZĄD MIEJSKI W TOSZKU
UL. BOLESŁAWA CHROBREGO 2
44-180 TOSZEK

INFORMATYK

Szymon Rabiza

Kierownik Referatu
Zamówień Publicznych,
Rozwoju i Promocji Gminy

mgr Iwona Filip


Adwokat
Aleksandra Piotrowska-Wnuk

Zastępca Burmistrza

mgr Piotr Kunce

SPIS TREŚCI

I. POSTANOWIENIA OGÓLNE.....	3
II. POJĘCIA UŻYWANE W NINIEJSZEJ INSTRUKCJI	4
III. PODSTAWA PRAWNA.....	5
IV. PROCEDURA NADAWANIA UPRAWNIENÍ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIENÍ W SYSTEMIE INFORMATYCZNYM.....	7
V. ZARZĄDZANIE SYSTEMEM HASEŁ	8
VI. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU	9
VII. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA	10
VIII. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH.....	11
IX. SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, O KTÓRYM MOWA W PKT III PPKT 1 ZAŁĄCZNIKA DO ROZPORZĄDZENIA.....	12
X. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH.....	14
XII. ZASADY KORZYSTANIA Z INTERNETU	15
XIII. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ	16
XIV. POSTANOWIENIA KOŃCOWE.....	17

I. POSTANOWIENIA OGÓLNE

Niniejszy dokument określa sposób zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych w Urzędzie Miejskim w Toszku (zwanego w dalszej części dokumentu „Urzędem”), w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnianiem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem, opisuje nadawanie uprawnień użytkownikom, określa sposoby pracy w systemie informatycznym oraz czynności mające wpływ na zapewnienie bezpieczeństwa systemu informatycznego.

II. POJĘCIA UŻYWANE W NINIEJSZEJ INSTRUKCJI

1. **Administrator danych osobowych (zwany dalej ADO)** oznacza osobę, która ustala cel(e) i sposoby przetwarzania danych osobowych. W omawianym przypadku ADO jest Urząd.
2. **Inspektor Ochrony Danych (zwany dalej IOD)** oznacza osobę, która nadzoruje przestrzeganie zasad ochrony danych osobowych, określonych przez ADO (zgodnie z wytycznymi określonymi w RODO).
3. **Administrator Systemu Informatycznego (zwany dalej ASI)** oznacza osobę odpowiedzialną za funkcjonowanie i bezpieczeństwo systemów informatycznych przetwarzających dane osobowe.
4. **Dane osobowe** oznaczają wszelkie informacje dotyczące jednostki, które pozwalają na jej identyfikację niezależnie od stosowanego środka komunikacji (np. papierowego, elektronicznego, video, audio). Przykładami danych osobowych są dane kontaktowe – imię i nazwisko, numer telefonu, numer PESEL, adresy IP, zdjęcia, historia przeglądania stron internetowych, geolokalizacja.
5. **Dane wrażliwe (inaczej szczególne kategorie danych)** oznaczają informacje dotyczące pochodzenia rasowego lub etnicznego; poglądów politycznych; przekonań religijnych lub innych przekonań światopoglądowych; przynależność do związków zawodowych; zdrowia fizycznego lub psychicznego; życia seksualnego; danych genetycznych; danych biometrycznych (np. pobieranie odcisków palców, system rozpoznawania rysów twarzy, skan siatkówki oka); informacje o popełnionych przestępstwach lub domniemanych przestępstwach popełnionych przez osobę, której dane dotyczą.
6. **Prezes Urzędu Ochrony Danych Osobowych (zwany dalej PUODO)** - jest organem do spraw ochrony danych osobowych działający na podstawie Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
7. **Obszar przetwarzania danych osobowych** – są to wszystkie miejsca w Urzędzie, gdzie dochodzi do przetwarzania danych osobowych. Obszar przetwarzania stanowią także lokalizacje podmiotu przetwarzającego dane, które Urząd powierza do przetwarzania.

8. **Naruszenie ochrony danych osobowych/naruszenie** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych (np. wiadomość e-mail zostaje nieumyślnie wysłana do nieprawidłowych adresatów, papierowy rejestr zostaje zgubiony lub ukradziony, cyberatak przeprowadzony przez hakerów).
9. **Przetwarzanie** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub nieautomatyzowany, 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.
10. **Podmiot przetwarzający (procesor)** oznacza podmiot zewnętrzny, który przetwarza dane osobowe w imieniu Urzędu (ADO) w celu zrealizowania przedmiotu umowy. Takimi podmiotami mogą być np. usługodawcy hostingu, BHP, usług serwisowych, firm archiwizujących bądź niszczących dokumenty.
11. **Profilowanie** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych w celu analizy lub prognozy osobowości lub niektórych cech osobowych odnoszących się do jednostki (np. analiza i prognoza zdrowia, sytuacji ekonomicznej, efektów pracy, lokalizacji, przemieszczania się, osobistych preferencji lub zainteresowań, zachowań w sieci takich jak historia przeglądania).
12. **Nośniki danych** – wszelkie nośniki, na których informacje zapisane są w postaci elektronicznej, w szczególności dyski, dyskietki, dyski CD-ROM, karty magnetyczne lub pamięci przenośne.
13. **Zbiór danych osobowych** – każdy posiadający strukturę logiczną zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

III. PODSTAWA PRAWNA

Instrukcja Zarządzania Systemem Informatycznym (zwana w dalszej części „Instrukcją”) została utworzona w związku z dobrą praktyką prowadzenia przez ADO dokumentacji

związanej z ochroną danych osobowych w oparciu o:

1. Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r. poz. 1000 z późn. zm.).
2. Rozporządzenie 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 (ogólne rozporządzenie o ochronie danych - RODO) – art.24.
3. Ustawę z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. z 2019 r. poz. 506).
4. Ustawę z dnia 21 listopada 2008 r. o pracownikach samorządowych (t.j. Dz.U. z 2018 r. poz. 1260).

IV. PROCEDURA NADAWANIA UPRAWNIENÍ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIENÍ W SYSTEMIE INFORMATYCZNYM

1. Każdy użytkownik systemu informatycznego przetwarzającego dane osobowe w Urzędzie przed przystąpieniem do przetwarzania danych osobowych winien zapoznać się z:
 - Polityką bezpieczeństwa danych osobowych,
 - Niniejszym dokumentem,oraz posiadać upoważnienie nadane przez ADO do przetwarzania danych osobowych (Zgodnie z Załącznikiem nr 2 Polityki bezpieczeństwa).
2. Zapoznanie się z powyższymi informacjami użytkownik potwierdza własnoręcznym podpisem na oświadczeniu pracownika przetwarzającego dane osobowe w momencie zatrudnienia (Zgodnie z Załącznikiem nr 1 Polityki bezpieczeństwa).
3. Powyższe Oświadczenie wraz z upoważnieniem do przetwarzania danych osobowych winno być przechowywane w teczce osobowej pracownika.
4. Praca w systemie informatycznym jest możliwa wyłącznie po uzyskaniu identyfikatora i hasła dostępu do sieci komputerowej i aplikacji.
5. Użytkownik ma prawo do wykonywania tylko tych czynności, do których został uprawniony.
6. Użytkownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
7. Modyfikacji uprawnień utworzonych wcześniej kont dokonuje ASI na podstawie wniosku o dokonanie modyfikacji uprawnień konta przesłanego za pośrednictwem poczty e-mail przez bezpośredniego przełożonego użytkownika systemu informatycznego.
8. Raz wyrejestrowanego identyfikatora użytkownika nie wolno przyznawać innym użytkownikom.

V. ZARZĄDZANIE SYSTEMEM HASEŁ

1. Bezpośredni dostęp do systemu informatycznego przetwarzającego dane osobowe może mieć miejsce wyłącznie po podaniu identyfikatora użytkownika oraz hasła.
2. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
3. Hasła użytkownika należy utrzymywać w tajemnicy również po upływie ich ważności.
4. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
5. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
6. Przy wyborze hasła obowiązują następujące zasady:
 - 7.1. Należy stosować:
 - 7.1.1. Hasła zawierające kombinacje liter i cyfr.
 - 7.1.2. Hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp.
 - 7.1.3. Hasła, które można zapamiętać bez zapisywania.
 - 7.1.4. Hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim.
 - 7.2. Zakazuje się stosować:
 - 7.2.1. Haseł, które użytkownik stosował uprzednio w okresie minionego roku.
 - 7.2.2. Swojej nazwy użytkownika w jakiegokolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.).
 - 7.2.3. Swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiegokolwiek formie.
 - 7.2.4. Imion (w szczególności imion osób z najbliższej rodziny).
 - 7.2.5. Ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy, na której mieszka lub pracuje, itp. wyrazów słownikowych.
 - 7.2.6. Przewidywalnych sekwencji znaków z klawiatury np.: QWERTY", "12345678", itp.
7. Zmiany hasła nie wolno zlecać innym osobom.
8. W systemach, które umożliwiają opcje zapamiętania nazw użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.

VI. PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZNACZONE DLA UŻYTKOWNIKÓW SYSTEMU

1. Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych.
2. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione oraz ogólne stwierdzenie poprawności działania systemu.
3. W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 15 minut winno nastąpić automatyczne zablokowanie systemu.
4. Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.
5. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, żeby uniemożliwić tym osobom wgląd w dane.
6. Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji.
7. Wszyscy użytkownicy mają obowiązek jak najszybszego zgłaszania wszelkich naruszeń zasad bezpieczeństwa systemów informatycznych, takich jak utratę haseł, ich ujawnienie lub podejrzenie o ich utracie.

VII. PROCEDURY TWORZENIA KOPII ZAPASOWYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada administrator systemu.
2. Kopie zapasowe wykonywane są automatycznie, po zakończeniu pracy przez użytkowników. Kopie zapasowe wykonywane są codziennie zgodnie z określoną konfiguracją przez ASI dla danej Aplikacji czy też Systemu Informatycznego.
3. Do tworzenia kopii zapasowych wykorzystywane są dedykowane do tego celu urządzenia wchodzące w skład systemu informatycznego.

VIII. SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA NOŚNIKÓW INFORMACJI ZAWIERAJĄCYCH DANE OSOBOWE ORAZ KOPII ZAPASOWYCH

1. Nośniki danych zarówno w postaci elektronicznej, jak i papierowej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem. Dane osobowe mogą być zapisywane na nośnikach przenośnych w przypadku tworzenia kopii zapasowych lub gdy istnieje konieczność przeniesienia tych danych w postaci elektronicznej, a wykorzystanie do tego celu sieci informatycznej jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.
2. Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafach wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej przyczyny wynoszone poza ten obszar. Przekazywanie nośników danych osobowych oraz wydruków poza budynku, w których mieści się siedziba i lokalizacje Urzędu powinno odbywać się za wiedzą ADO.
3. W przypadku, gdy nośnik danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie nośnika lub usunięcie danych z nośnika. Jeżeli wydruk danych osobowych nie jest dłużej potrzebny, należy przeprowadzić zniszczenie wydruku przy użyciu niszcarki dokumentów.
4. W przypadku, gdy kopia zapasowa nie jest dłużej potrzebna, należy przeprowadzić jej zniszczenie lub usunięcie danych z nośnika.

**IX. SPOSÓB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZED
DZIAŁALNOŚCIĄ OPROGRAMOWANIA, O KTÓRYM MOWA W PKT III PPKT 1
ZAŁĄCZNIKA DO ROZPORZĄDZENIA**

1. W związku z narażeniem systemu informatycznego na działanie oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu konieczne jest podjęcie odpowiednich środków ochronnych.
2. Można wyróżnić następujące rodzaje występujących zagrożeń:
 - 2.1 Nieuprawniony dostęp bezpośrednio do bazy danych.
 - 2.2 Uszkodzenie kodu aplikacji umożliwiającej dostęp do bazy danych w taki sposób, że przetwarzane dane osobowe ulegną zafałszowaniu lub zniszczeniu.
 - 2.3 Przechwycenie danych podczas transmisji w przypadku rozproszonego przetwarzania danych z wykorzystaniem ogólnodostępnej sieci Internet.
 - 2.4 Przechwycenie danych z aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych przez wyspecjalizowany program szpiegowski i nielegalne przesłanie tych danych poza miejsce przetwarzania danych.
 - 2.5 Uszkodzenie lub sfałszowanie danych osobowych przez wirus komputerowy zakłócający pracę aplikacji umożliwiającej dostęp do bazy danych na stacji roboczej wykorzystywanej do przetwarzania danych osobowych.
3. W celu przeciwdziałania wymienionym zagrożeniom system informatyczny musi posiadać następujące zabezpieczenia:
 - 3.1. Fizyczne odseparowanie serwera bazy danych od publicznej sieci zewnętrznej.
 - 3.2. Autoryzacja użytkowników przy zachowaniu odpowiedniego poziomu komplikacji haseł dostępu.
 - 3.3. Stosowanie rygorystycznego systemu autoryzacji dostępu do wszystkich serwerów, na których znajdują się elementy aplikacji umożliwiających przetwarzanie danych osobowych.
 - 3.4. Stosowanie odpowiedniej ochrony antywirusowej na stacjach roboczych wykorzystywanych do przetwarzania danych osobowych.

4. Potencjalnymi źródłami przedostawania się programów szpiegowskich oraz wirusów komputerowych na stacje robocze są załączniki do poczty elektronicznej, przeglądane strony internetowe oraz pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.
5. W celu zapewnienia ochrony antywirusowej ASI, lub osoba specjalnie do tego celu wyznaczona, jest odpowiedzialna za zarządzanie systemem wykrywającym i usuwającym wirusy.
6. System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.
7. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy ASI lub inny wyznaczony pracownik powinien podjąć działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
 - 7.1. Usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego.
 - 7.2. Odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane.
 - 7.3. Samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z zewnętrznymi ekspertami.
8. System informatyczny przetwarzający dane osobowe powinien posiadać mechanizmy pozwalające na zabezpieczenie ich przed utratą lub wystąpieniem zafałszowania w wyniku awarii zasilania lub zakłóceń w sieci zasilającej. W związku z tym system informatyczny powinien być wyposażony w co najmniej:
 - 8.1. Filtry zabezpieczające stacje robocze przed skutkami przepięcia.
 - 8.2. Zasilacze awaryjne serwerów baz danych, serwerów aplikacji oraz urządzeń pamięci masowej pozwalające na bezpieczne zamknięcie aplikacji przetwarzających dane osobowe w sposób umożliwiający poprawne zapisanie przetwarzanych danych.

X. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
2. Prace serwisowe w siedzibie Urzędu prowadzone w tym zakresie mogą być wykonywane wyłącznie przez osoby zatrudnione w Urzędzie lub przez upoważnionych przedstawicieli wykonawców zewnętrznych nadzorowanych przez pracowników Urzędu.
3. Przed rozpoczęciem prac serwisowych przez osoby niezatrudnione w Urzędzie konieczne jest potwierdzenie tożsamości serwisantów. W przypadku stałej współpracy należy podpisać umowę powierzenia przetwarzania danych osobowych.
4. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
 - 4.1. Likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.
 - 4.2. Przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie.
 - 4.3. Naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez ADO.

XII. ZASADY KORZYSTANIA Z INTERNETU

1. Każdy pracownik Urzędu zobowiązany jest do korzystania z Internetu głównie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie ściągnięte z Internetu i przez niego zainstalowane.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym lub innym zakazanym przez prawo (istnieje niebezpieczeństwo, iż na stronach tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. Należy korzystać z następujących przeglądarek Internetu:
 - 6.1. Google Chrome.
 - 6.2. Mozilla Firefox.
 - 6.3. Microsoft Internet Explorer.
 - 6.4. Apple Safari.
7. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka, protokół https).

XIII. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. W przypadku przesyłania informacji szczególnie poufnych, w tym takich które zawierają dane osobowe należy wykorzystywać mechanizmy kryptograficzne (pakowanie i hasłowanie wysyłanych plików, podpis elektroniczny itp.).
2. Należy zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
3. Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
4. Użytkownicy nie powinni rozsyłać za pośrednictwem poczty elektronicznej informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia” itp.

XIV. POSTANOWIENIA KOŃCOWE

1. Wszyscy pracownicy Urzędu są zobowiązani do zapoznania się z treścią niniejszej Instrukcji.
2. Instrukcja wchodzi w życie z dniem podpisania.

KARTA KOMPUTERA

Komputer Stacjonarny	
Element konfiguracji	Czy konfiguracja zawiera wymieniony element? (opis i rodzaj)
Procesor(y)	
Płyta główna	
Karta graficzna	
Karta dźwiękowa	
Pamięć RAM	
Dysk twardy	
Napęd dyskietek FDD	
Napęd optyczny	
Karty sieciowe	
Modem	
Porty zewnętrzne	
Obudowa	
Zasilacz	
Mysz	
Klawiatura	
Monitor	
Oprogramowanie	
Gwarancja	
Inne	

Osoba pracująca przy komputerze jest odpowiedzialna za zgłaszanie wszelkich błędów związanych z nim do Informatyka Urzędu Miejskiego w Toszku.

.....
Podpis osoby pracującej
z komputerem

.....
Informatyk
Urzędu Miejskiego w Toszku

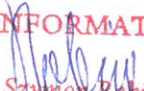
**WNIOSEK O NADANIE/ ZMIANĘ/ USUNIĘCIE UPRAWNIEŃ W SYSTEMIE
INFORMATYCZNYM***

Urząd Miejski w Toszku

Nowy użytkownik ☐	Modyfikacja uprawnień ☐	Usunięcie uprawnień ☐
---	---	---

Imię i nazwisko użytkownika	Komórka organizacyjna/samodzielne stanowisko
Opis zakresu uprawnień użytkownika w systemie informatycznym	
Data wystawienia:	Podpis bezpośredniego przełożonego użytkownika systemu informatycznego:
Zgoda ADO:	

*Wniosek należy złożyć do ASI

INFORMATYK

Szymon Rabiza

**POLITYKA
CZYSTEGO BIURKA I CZYSTEGO EKRANU**

1. Niniejsza „Polityka czystego biurka i czystego ekranu” (dalej: „Polityka”) Urzędu Miejskiego w Toszku (dalej: „Urząd”) obowiązuje wszystkich pracowników.
2. Przez pracownika Urzędu należy rozumieć osobę, o której mowa w art. 2 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz.U. z 2019 r. poz. 1040), tj. osobę zatrudnioną na podstawie umowy o pracę, powołania, wyboru, mianowania lub spółdzielczej umowy o pracę, a także wszystkie pozostałe osoby, które wykonują pracę na innej podstawie prawnej niż stosunek pracy (w tym osoby przyjęte na praktyki), a także osoby współpracujące prowadzące jednoosobową działalność gospodarczą.
3. Zgodnie z niniejszą Polityką każdy pracownik:
 - zobowiązany jest do przechowywania na biurku tylko tych dokumentów, jakie są mu niezbędne do realizacji bieżących zadań;
 - po zakończonej pracy zobowiązany jest do zabezpieczenia dokumentów w zamykanej na klucz szafie. Klucz do szafy należy zdeponować w przeznaczonym do tego miejscu lub przekazać innemu pracownikowi, na którego przechodzi odpowiedzialność za realizację Polityki;
 - zobowiązany jest do niszczenia na bieżąco dokumentów, które przestały być potrzebne, w sposób uniemożliwiający odtworzenie zawartych w nich informacji, np. w niszczarce;
 - nie powinien przechowywać na biurku wszelkich produktów spożywczych, które mogą ulec rozlaniu;
 - jest zobowiązany do ustawienia wygaszacza ekranu na użytkowanym komputerze zabezpieczonego hasłem. W przypadku czasowego opuszczenia stanowiska pracy, pracownik zobowiązany jest do blokowania komputera poprzez uruchomienie wygaszacza;

Kierownik Referatu
Zamówień Publicznych,
Rozwoju i Promocji Gminy

mgr Iwona Filip

INFORMATYK

Szymon Kubiś

Adwokat

Aleksandra Piotrowska-Wnuk

Zastępca Burmistrza

mgr Piotr Kunce

Urząd Miejski w Toszku

- powinien dopilnować, aby monitor komputera skierowany był w jego stronę i uniemożliwiać odczytywanie z niego danych przez osoby nieupoważnione;
 - powinien wylogować się z systemu po zakończeniu pracy;
 - powinien pozostawić po zakończonej pracy jedynie niezbędne materiały biurowe czy sprzęt komputerowy.
4. Podstawą prawną niniejszej Polityki jest art. 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 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 nazywanego ogólnym Rozporządzeniem o ochronie danych osobowych.

Oświadczam, iż zapoznałem się z powyższą Polityką czystego biurka i ekranu i zobowiązuję się do jej stosowania.

.....
(podpis składającego oświadczenie)

PROCEDURA DOSTĘPU DO DANYCH NA ŻĄDANIE OSOBY

1. Cel procedury

1.1. Zapewnienie osobie fizycznej możliwości realizacji prawa do:

1.1.1. Uzyskania potwierdzenia, czy przetwarzane są jej dane osobowe, a jeżeli ma to miejsce, do uzyskania dostępu do nich.

1.1.2. Uzyskania informacji na temat przetwarzania jej danych osobowych.

2. Stosowanie procedury

2.1. Procedura ma zastosowanie, gdy osoba zgłosi żądanie dostępu do swoich danych lub informacji na temat przetwarzania jej danych osobowych.

3. Opis postępowania

3.1. Realizacja żądania

3.1.1. Rozpatrywanie żądania

3.1.1.1. Po otrzymaniu żądania należy zidentyfikować osobę przez uprawnionego pracownika Urzędu. W przypadku, gdy podane w żądaniu dane nie są wystarczające do identyfikacji (gdy istnieją uzasadnione wątpliwości co do tożsamości osoby), należy skontaktować się z tą osobą w celu uzyskania dodatkowych informacji pozwalających na jej identyfikację, np. nr PESEL.

3.1.1.2. Podczas rozpatrywania żądania należy ustalić stan faktyczny. W tym uprawniony pracownik Urzędu rozpatrujący żądanie ma prawo kontaktować się z dowolnym pracownikiem Urzędu mającym dostęp do danych osobowych i otrzymać niezbędne informacje.

3.1.1.3. Pracownik, który otrzymał zapytanie dotyczące realizacji żądania dostępu do danych ma obowiązek przekazania niezwłocznie żądanych informacji (np. kopii dokumentów, zrzutów ekranu) a także udzielić dostępu do systemu informatycznego itp.

3.1.2. Udzielenie odpowiedzi

3.1.2.1. Następnie należy przygotować odpowiedź na wniesione żądanie zawierające następujące informacje:

- W przypadku żądania dotyczącego potwierdzenia przetwarzania danych osobowych – potwierdzenie lub brak potwierdzenia w oparciu o ustalony stan faktyczny;

Kierownik Referatu
Zamówień Publicznych,
Rozwoju i Promocji Gminy

mgr Iwona Filip

INFORMATYK

Szymon Rabiza

Adwokat

Aleksandra Piotrowska-Wnuk

Zastępca Burmistrza
mgr Piotr Kunce

Urząd Miejski w Toszku

- W przypadku żądania dotyczącego przekazania informacji o przetwarzaniu danych osobowych – ustalenia dotyczące informacji w zakresie objętym żądaniem Osoby. Osoba ma prawo do następujących informacji:
 - cele przetwarzania,
 - kategorie danych osobowych,
 - informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
 - w miarę możliwości planowany okres przechowywania danych, a gdy nie jest to możliwe, kryteria ustalanie tego okresu,
 - informacje o prawie żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
 - informacje o prawie wniesienia skargi do organu nadzorczego,
 - jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle,
 - informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą,
 - jeśli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej o odpowiednich zabezpieczeniach związanych z przekazaniem danych.
- W przypadku żądania dotyczącego dostępu do danych osobowych należy:
 - ustalić, do której grupy osób należy osoba (np. pracownicy, klienci, kandydaci do pracy, itp.), w których systemach informatycznych oraz na jakich formularzach papierowych są zapisane i przechowywane dane osoby
 - jeśli przetwarzane są duże ilości informacji o osobie, można zażądać przed podaniem informacji, by osoba sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie
 - przygotować odpowiednie wydruki, zestawienia, raporty z systemów informatycznych oraz kopie dokumentów, formularzy zawierających dane osoby lub umożliwić osobie zdalny dostęp do bezpiecznego systemu, który zapewni bezpośredni dostęp do jej danych osobowych
 - sprawdzić czy na kopiach i wydrukach udostępnionych osobie nie znajdują się dane innych osób lub informacje będące tajemnicą handlową lub własność intelektualna. Z kopii, wydruków lub systemu muszą zostać usunięte ww. Informacje.

**PROCEDURA POSTĘPOWANIA W RAZIE ZAISTNIENIA NARUSZENIA
PRZETWARZANIA DANYCH OSOBOWYCH**

1. Incydem naruszającym bezpieczeństwo przetwarzania danych osobowych jest każde pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem przetwarzanych danych osobowych, które stwarzają znaczne prawdopodobieństwo zakłócenia prawidłowego przetwarzania danych.
2. Incydenty przetwarzania danych osobowych mogą dotyczyć następujących obszarów:
 - 2.1. Zabezpieczenia systemu informatycznego.
 - 2.2. Technicznego stanu urządzeń.
 - 2.3. Zawartości zbioru danych osobowych.
 - 2.4. Ujawnienia metody pracy lub sposobu działania programu.
 - 2.5. Jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych.
 - 2.6. Innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.).
3. W przypadku podejrzenia lub stwierdzenia naruszenia ochrony danych osobowych ma zastosowanie następująca procedura:
 - 3.1. Każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić o tym bezpośredniego przełożonego, informatyka bądź inną osobę mogącą podejmować decyzje w kwestii bezpieczeństwa.
 - 3.2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych osoby określonej w p. 3.1. należy:
 - 3.2.1. Niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców.

Kierownik Referatu
Zamówień Publicznych,
Rozwoju i Promocji Gminy
mgr Iwona Filip

INFORMATYK
Szymon Rabiza

Aleksandra Piotrowska-Wnuk
Adwokat

Zastępca Burmistrza
mgr Piotr Kunce

Urząd Miejski w Toszku

- 3.2.2. Rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia.
- 3.2.3. Zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę.
- 3.2.4. Podjąć odpowiednie działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej.
- 3.2.5. Nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia osoby określonej w p. 3.1.
- 3.3. Po przybyciu na miejsce zdarzenia osoba upoważniona:
 - 3.3.1. Zapoznać się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy.
 - 3.3.2. Może żądać dokładnej relacji z zaistniałego incydentu od osoby powiadamiającej.
 - 3.3.3. Może również zażądać relacji od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem.
 - 3.3.4. Jeśli zachodzi taka konieczność nawiązuje bezpośredni kontakt ze specjalistami spoza Urzędu.
- 3.4. Osoba uprawniona (np. określona w p. 3.1.) dokumentuje zaistniały przypadek naruszenia w rejestrze naruszeń wg obowiązującego w Urzędzie wzoru (stanowiącego załącznik nr 7 do Polityki bezpieczeństwa), który zawiera:
 - 3.4.1. Określenie czasu i miejsca naruszenia.
 - 3.4.2. Określenie okoliczności towarzyszących i rodzaju naruszenia.
 - 3.4.3. Skutki naruszenia.
 - 3.4.4. Opis przeprowadzonego postępowania wyjaśniającego i naprawczego.
 - 3.4.5. Określenie czy naruszenie podlega obowiązkowi powiadomienia do Organu Nadzoru.
- 3.5. Jeśli naruszenie i jego ewentualne skutki wymagają zgłoszenia tego faktu do Organu Nadzoru, należy powiadomić na drodze pisemnej Organ Nadzoru (Urząd Ochrony Danych Osobowych) w ciągu 72 godzin od stwierdzenia naruszenia. Zgłoszenie to będzie możliwe do zrealizowania poprzez formularz dostępny na stronie internetowej Urzędu (<https://uodo.gov.pl/pl/134/233>).

Urząd Miejski w Toszku

Osobą odpowiedzialną za zgłoszenie jest **Administrator Danych Osobowych wraz z Inspektorem Ochrony Danych**.

- 3.6. Jeśli naruszenie dotyczy osoby fizycznej i spowodowało utratę bądź nieuprawnione ujawnienie jej danych należy tę osobę o fakcie naruszenia jej danych powiadomić.
4. Najczęstsze przypadki incydentów związanych z przetwarzaniem danych osobowych:
 - 4.1. Naruszenie zabezpieczeń systemu informatycznego bądź oprogramowania przetwarzającego dane osobowe.
 - 4.2. Naruszenie technicznego stanu urządzeń służących do przetwarzania danych osobowych.
 - 4.3. Naruszenie zawartości zbioru danych osobowych.
 - 4.4. Ujawnienie metody pracy lub sposobu działania programu osobie nieupoważnionej do przetwarzania danych osobowych.
 - 4.5. Kradzież danych osobowych (zapisanych na nośniku, komputerze, dokumentach papierowych).
 - 4.6. Zagubienie bądź wyrzucenie danych osobowych, które pracownik przetwarzał.
 - 4.7. Omyłkowe ujawnienie danych osobowych osobie nieupoważnionej (np. poprzez wysyłkę pocztą elektroniczną danych osobowych do niewłaściwego adresata).
 - 4.8. Inne zdarzenia mogące mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.).

PROCEDURA REALIZACJI PRAWA DO OGRANICZENIA PRZETWARZANIA

1. Cel procedury

- 1.1. Zapewnienie Osobom możliwości realizacji prawa do ograniczenia przetwarzania danych.

2. Stosowanie procedury

- 2.1. Procedura ma zastosowanie, gdy osoba fizyczna zgłosi żądanie ograniczenia przetwarzania danych (Żądanie).

3. Opis postępowania

3.1. Realizacja żądania

- 3.1.1. Po otrzymaniu żądania należy zidentyfikować osobę przez uprawnionego pracownika Urzędu. W przypadku, gdy podane w żądaniu dane nie są wystarczające do identyfikacji (gdy istnieją uzasadnione wątpliwości co do tożsamości osoby), należy skontaktować się z tą osobą w celu uzyskania dodatkowych informacji pozwalających na jej identyfikację, np. nr PESEL.
- 3.1.2. Po otrzymaniu żądania należy zweryfikować jego zasadność uwzględniając informacje z pkt 4 poniżej „Ograniczenie przetwarzania danych – przesłanki stosowania”.
- 3.1.3. Jeśli żądanie nie jest zasadne należy przygotować odpowiedź o odmowie uwzględnienia żądania.
- 3.1.4. Jeśli żądanie osoby jest zasadne uprawniony pracownik rozpatrujący żądanie przekazuje polecenie:
- pracownikom, u których dane są przechowywane lub które korzystają z dokumentów papierowych zawierających dane osobowe,
 - podmiotom, którym dane zostały udostępnione lub powierzone do przetwarzania
- oznaczenia ograniczenia przetwarzania danych Osoby - w zakresie zgodnym z żądaniem osoby oraz wskazuje termin, po którym będzie możliwe dalsze przetwarzanie danych bez ograniczenia (uchylenie ograniczenia przetwarzania).

- 3.1.5. Należy archiwizować wszelkie kopie udzielonych odpowiedzi wraz z datą ich udzielenia.

- 3.1.6. Przed uchyleniem ograniczenia przetwarzania należy o tym fakcie poinformować o tym osobę wnoszącą żądanie.

Kierownik Referatu
Zamówień Publicznych,
Rozwoju i Promocji Gminy

mgr Iwona Filip

INFORMATYK

Szymon Raluza

Adwokat

Aleksandra Piotrowska-Wnuk

Zastępca Burmistrza
mgr Piotr Kunce

4. Ograniczenie przetwarzania danych – przesłanki stosowania

- 4.1. Osoba ma prawo żądać ograniczenia przetwarzania swoich danych otrzymać w następujących przypadkach:
- 4.1.1. Osoba kwestionuje prawidłowość danych - na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
 - 4.1.2. Przetwarzanie jest niezgodne z prawem, a Osoba sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
 - 4.1.3. Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne Osobie do ustalenia, dochodzenia lub obrony roszczeń;
 - 4.1.4. Osoba wniosła sprzeciw na mocy Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE art. 21 ust. 1 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
- 4.2. Jeżeli w wyniku żądania Osoby przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

PROCEDURA REALIZACJI PRAWA DO PRZENOSZENIA DANYCH

1. Cel procedury

- 1.1. Zapewnienie osobom możliwości realizacji prawa do przenoszenia danych.

2. Stosowanie procedury

- 2.1. Procedura ma zastosowanie, gdy osoba fizyczna zgłosi żądanie realizacji prawa do przenoszenia danych.

3. Opis postępowania

3.1. Realizacja żądania

- 3.1.1. Po otrzymaniu żądania należy zidentyfikować osobę przez uprawnionego pracownika Urzędu. W przypadku, gdy podane w żądaniu dane nie są wystarczające do identyfikacji (gdy istnieją uzasadnione wątpliwości co do tożsamości osoby), należy skontaktować się z osobą w celu uzyskania dodatkowych informacji pozwalających na jej identyfikację, np. nr PESEL.
- 3.1.2. Po otrzymaniu żądania należy zweryfikować jego zasadność uwzględniając informacje z pkt 4 poniżej „Ograniczenie przetwarzania danych – przesłanki stosowania”.
- 3.1.3. Jeśli żądanie nie jest zasadne należy przygotować odpowiedź o odmowie uwzględnienia żądania.
- 3.1.4. Jeśli Żądanie jest zasadne, administrator systemów informatycznych Urzędu, w których zapisane są dane osoby przygotowanie danych osobowych do przekazania osobie lub innemu administratorowi, lub wykonuje to osobiście – zgodnie z żądaniem osoby.
- 3.1.5. Dane osoby przygotowane do przekazania muszą spełniać wymogi określone w pkt. 4.1. poniżej.
- 3.1.6. IOD przekazuje dane osobie lub innemu administratorowi – zgodnie z wniesionym żądaniem.
- 3.1.7. Należy dokumentować deka przekazania danych Osoby wraz z datą przekazania oraz sposobem wykonania Żądania.

4. Przeniesienie danych – przesłanki stosowania

- 4.1. Każda osoba fizyczna ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące oraz ma prawo przesłać te dane osobowe innemu administratorowi

Kierownik Referatu
Zamówień Publicznych,
Rozwoju i Promocji Gminy

mgr Iwona Filip

INFORMATYK

Szymon Kubiś

Adwokat

Aleksandra Piotrowska-Wnuk

Zastępca Burmistrza
mgr Piotr Kunc

Urząd Miejski w Toszku

bez przeszkód ze strony Administratora, jeżeli spełnione są łącznie następujące przesłanki:

- 4.1.1. Przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy.
- 4.1.2. Przetwarzanie odbywa się w sposób zautomatyzowany.
- 4.2. Osoba ma prawo żądania, by dane osobowe zostały przesłane bezpośrednio innemu administratorowi. Obowiązek ten należy zrealizować, o ile jest to technicznie możliwe.
- 4.3. Przeniesienie danych dotyczy tylko tych danych, które osoba samodzielnie dostarczyła Administratorowi. Nie należy przenosić danych, które zostały pozyskane z innych źródeł.
- 4.4. Przeniesienie danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.
- 4.5. Realizując prawo do przeniesienia danych, nie można niekorzystnie wpływać na prawa i wolności innych osób.

PROCEDURA REALIZACJI PRAWA DO SPROSTOWANIA DANYCH

1. Cel procedury

1.1. Zapewnienie Osobom, których dane dotyczą, możliwości realizacji prawa do:

1.1.1. Niezwłocznego sprostowania danych osobowych lub

1.1.2. Uzupełnienia niekompletnych danych osobowych

2. Stosowanie procedury

2.1. Procedura ma zastosowanie w przypadku, gdy Osoba zgłosi żądanie niezwłocznego sprostowania nieprawidłowych danych osobowych lub uzupełnienia niekompletnych danych osobowych, które jej dotyczą.

3. Opis realizacji

3.1. Realizacja żądania:

3.1.1. Po otrzymaniu żądania należy zidentyfikować osobę przez uprawnionego pracownika Urzędu. W przypadku, gdy podane w żądaniu dane nie są wystarczające do identyfikacji (gdy istnieją uzasadnione wątpliwości co do tożsamości osoby), należy skontaktować się z tą osobą w celu uzyskania dodatkowych informacji pozwalających na jej identyfikację, np. nr PESEL.

3.1.2. Po otrzymaniu żądania należy zweryfikować jego zasadność uwzględniając informacje z pkt 4 poniżej – „Obowiązek sprostowania lub uzupełnienia danych – przesłanki stosowania”.

3.1.3. Jeśli żądanie nie jest zasadne należy przygotować odpowiedź o odmowie uwzględnienia żądania.

3.1.4. Jeśli żądanie jest zasadne należy je rozpatrzyć przez ustalenie, w których systemach, aplikacjach, programach lub dokumentach prowadzonych w formie papierowej należy sprostować lub uzupełnić niekompletne dane osoby.

3.1.5. Identyfikacja wszystkich miejsc w których zapisane są dane osoby oznacza również konieczność ustalenia ich przetwarzania przez podmioty, którym dane zostały udostępnione lub przekazane do przetwarzania oraz powiadomienie tych podmiotów o konieczności sprostowania lub uzupełnienia niekompletnych danych zgodnie z żądaniem.

3.1.6. Następnie należy przygotować odpowiedź na wniesione żądanie informującą o sprostowaniu lub uzupełnieniu niekompletnych danych wraz z podaniem terminu, w którym dane zostały sprostowane i/lub uzupełnione.

Kierownik Referatu
Zamówień Publicznych,
Rozwoju i Promocji Gminy
mgr Iwona Filip

INFORMATYK

Szymon Rabiza

Adwokat

Aleksandra Piotrowska-Wnuk

Zastępca Burmistrza

mgr Piotr Kunce

Urząd Miejski w Toszku

3.1.7. Należy archiwizować kopie udzielonych odpowiedzi wraz z datą ich udzielenia.

4. Obowiązek sprostowania i/lub uzupełnienia danych – przesłanki stosowania

4.1. Prawo do sprostowania lub uzupełnienia danych musi zostać zrealizowane, jeśli zachodzi jedna z następujących okoliczności:

4.1.1. Nastąpiła zmiana danych osobowych.

4.1.2. Przetwarzane uprzednio dane osobowe były nieprawidłowe.

4.1.3. Przetwarzane uprzednio dane były niekompletne.

PROCEDURA REALIZACJI PRAWA DO SPRZECIWU

1. Cel procedury

- 1.1. Zapewnienie osobom fizycznym możliwości realizacji prawa do wniesienia sprzeciwu wobec przetwarzania jej danych osobowych.

2. Stosowanie procedury

- 2.1. Procedura ma zastosowanie, gdy osoba wniesie sprzeciw wobec przetwarzania jej danych osobowych (żądanie).

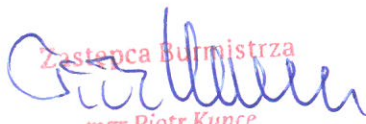
3. OPIS POSTĘPOWANIA

3.1. Realizacja Żądania

- 3.1.1. Po otrzymaniu żądania należy zidentyfikować osobę przez uprawnionego pracownika Urzędu. W przypadku, gdy podane w żądaniu dane nie są wystarczające do identyfikacji (gdy istnieją uzasadnione wątpliwości co do tożsamości osoby), należy skontaktować się z tą osobą w celu uzyskania dodatkowych informacji pozwalających na jej identyfikację, np. nr PESEL.
- 3.1.2. Po otrzymaniu żądania należy zweryfikować jego zasadność uwzględniając informacje z pkt 4 poniżej „Sprzeciw wobec przetwarzania danych – przesłanki stosowania” oraz ustalając cele, w których są przetwarzane dane Osoby.
- 3.1.3. Jeśli żądanie nie jest zasadne należy przygotować odpowiedź o odmowie uwzględnienia żąda
- 3.1.4. Jeśli żądanie jest zasadne należy zaprzestać dalszego przetwarzania danych osoby – zgodnie z jej żądaniem oraz należy podjąć działania mające na celu zapobiegnięcie możliwości dalszego przetwarzania danych. Polecenie zaprzestania dalszego przetwarzania należy przekazać również podmiotom, którym dane osobowe zostały udostępnione lub powierzone do przetwarzania.
- 3.1.5. Należy następnie przygotować odpowiedź na żądanie osoby z informacją o zaprzestaniu przetwarzania jej danych wraz z podaniem terminu, w którym dane przestaną być przetwarzane.
- 3.1.6. Należy archiwizować kopie udzielonych odpowiedzi wraz z datą ich udzielenia.

4. Sprzeciw wobec przetwarzania danych – przesłanki

- 4.1. Sprzeciw na przetwarzanie danych w celach marketingu bezpośredniego, w tym profilowania

Zastępca Burmistrza

mgr Piotr Kunce

Kierownik Referatu
Zamówień Publicznych,
Rozwoju i Promocji Gminy
Adwokat
Sędzią
Piotrowska-Wojcik Iwona Filip
INFORMATYK
Szymon Babiza

Urząd Miejski w Toszku

- 4.1.1. Osoba posiada prawo wniesienia sprzeciwu wobec przetwarzania jej danych w dowolnym momencie, a Administratorowi nie wolno już przetwarzać danych w tych celach.
- 4.2. Sprzeciw na przetwarzanie danych na podstawie prawnie uzasadnionego interesu administratora lub strony trzeciej oraz w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi
 - 4.2.1. Osoba posiada prawo wniesienia sprzeciwu - ze względu na jej szczególną sytuację - wobec przetwarzania jej danych w dowolnym momencie, a Administratorowi nie wolno już przetwarzać danych w tych celach, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności Osoby lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
- 4.3. Sprzeciw na przetwarzanie danych do celów badań naukowych lub historycznych lub do celów statystycznych.
 - 4.3.1. Osoba posiada prawo wniesienia sprzeciwu - ze względu na jej szczególną sytuację - wobec przetwarzania jej danych, a Administratorowi nie wolno już przetwarzać danych w tych celach, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

PROCEDURA REALIZACJI PRAWA DO USUNIĘCIA DANYCH - „PRAWO DO BYCIA ZAPOMNIANYM”

1. Cel procedury

- 1.1. Celem procedury jest zapewnienie osobom, których dane dotyczą, możliwości realizacji prawa do usunięcia jej danych.

2. Stosowanie procedury

- 2.1. Procedura ma zastosowanie, gdy osoba fizyczna zgłosi żądanie realizacji prawa do usunięcia dotyczących jej danych osobowych.

3. Opis postępowania

3.1. Realizacja Żądania

- 3.1.1. Po otrzymaniu żądania należy zidentyfikować osobę składającą żądanie przez uprawnionego pracownika Urzędu. W przypadku, gdy podane w żądaniu dane nie są wystarczające do identyfikacji (gdy istnieją uzasadnione wątpliwości co do tożsamości osoby), należy skontaktować się z tą osobą w celu uzyskania dodatkowych informacji pozwalających na jej identyfikację, np. nr PESEL, nr umowy itp.
- 3.1.2. Po otrzymaniu żądania należy zweryfikować jego zasadność uwzględniając informacje z pkt 4 poniżej „Obowiązek usunięcia danych – przesłanki stosowania”.
- 3.1.3. Jeśli żądanie nie jest zasadne należy przygotować odpowiedź o odmowie uwzględnienia żądania.
- 3.1.4. Jeśli żądanie jest zasadne należy ustalić wszystkie formy i miejsca przetwarzania danych osoby (np. aplikacje i systemy informatyczne, zewnętrzne nośniki danych, formularze papierowe). W tym celu należy kontaktować się z każdym pracownikiem Urzędu mającym dostęp do danych osobowych i otrzymać niezbędne informacje.
- 3.1.5. Następnie należy przygotować odpowiedź na żądanie osoby z informacją o usunięciu danych wraz z podaniem terminu, w którym dane zostaną lub zostały usunięte.
- 3.1.6. Należy archiwizować wszelkie kopie udzielonych odpowiedzi wraz z datą ich udzielenia.
- 3.1.7. Po zidentyfikowaniu wszystkich miejsc, w których są zapisane dane osoby należy je usunąć. Identyfikacja wszystkich miejsc w których zapisane są dane osoby oznacza również konieczność ustalenia ich przetwarzania przez

Kierownik Referatu
Zamówień Publicznych,
Wydział Promocji Gminy
mgr Iwona Filip

Adwokat
Aleksandra Piotrowska-Wądek

INFORMATYK
Szymon Rabiza

Zastępca Burmistrza
mgr Piotr Kunce

podmioty, którym dane zostały udostępnione lub przekazane do przetwarzania oraz powiadomienie tych podmiotów o konieczności usunięcia danych.

3.1.8. Usunięciu nie podlegają:

- Żądanie Osoby;
- formularz, na którym zostało zapisane Żądanie Osoby przez pracownika przyjmującego Żądanie;
- udzielona odpowiedź.

4. Obowiązek usunięcia danych osobowych/prawa do bycia zapomnianym – przesłanki stosowania

4.1. Prawo do usunięcia danych musi zostać zrealizowane, jeśli zachodzi jedna z następujących okoliczności:

- 4.1.1. Dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane.
- 4.1.2. Osoba cofnęła zgodę na przetwarzanie jej danych osobowych i nie ma innej podstawy prawnej przetwarzania.
- 4.1.3. W przypadku przetwarzania dokonywanego w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi, jak również w celu wynikającym z prawnie uzasadnionych interesów Administratora – gdy Osoba wnosi sprzeciw wobec przetwarzania z przyczyn związanych z jej szczególną sytuacją i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania.
- 4.1.4. W przypadku przetwarzania danych na potrzeby marketingu bezpośredniego, w tym profilowania – gdy Osoba wnosi sprzeciw wobec przetwarzania.
- 4.1.5. Dane osobowe były przetwarzane niezgodnie z prawem.
- 4.1.6. Dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w powszechnie obowiązujących przepisach.
- 4.1.7. Dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.

4.2. Obowiązek usunięcia danych oraz poinformowania innych administratorów, nie ma zastosowania w takim zakresie, w jakim przetwarzanie jest niezbędne:

- 4.2.1. Do korzystania z prawa do wolności wypowiedzi i informacji.
- 4.2.2. Do wywiązania się z prawnego obowiązku wymagającego przetwarzania zgodnie z powszechnie obowiązującymi przepisami lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.
- 4.2.3. Z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego.

Urząd Miejski w Toszku

4.2.4. Do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych podlegającym odpowiednim zabezpieczeniom dla praw i wolności osób, których dane dotyczą, o ile prawdopodobne jest, że usunięcie danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania

lub

4.2.5. Do ustalenia, dochodzenia lub obrony roszczeń.

INFORMATYK


Szymon Rabiza

1. Niniejsze „Zasady użytkowania urządzeń mobilnych” (dalej: Zasady) są częścią Polityki Bezpieczeństwa Danych Osobowych i obowiązują wszystkich pracowników Urzędu Miejskiego w Toszku (zwanego dalej: „Urzędem”), którzy przetwarzają informacje poufne w tym dane osobowe za pomocą powierzonych im urządzeń mobilnych.
2. Przez urządzenia mobilne należy rozumieć: laptopy, tablety, telefony komórkowe, smartfony, smartwatche.
3. Osoby korzystające z urządzeń mobilnych i systemu informatycznego zobowiązane są do:
 - Zabezpieczenia za pomocą hasła, PIN-u, wzoru dotykowego lub informacji biometrycznych (w tym odcisku palca, skanu twarzy) przekazanego urządzenia mobilnego.
 - Posługiwania się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych.
 - Tworzenia haseł trudnych do odgadnięcia, składających się z małych i dużych liter, zawierających co najmniej jedną cyfrę i znak specjalny.
 - Nieujawniania loginu i hasła dostępu do urządzeń mobilnych współpracownikom, a także innym osobom nieuprawnionym, w tym członkom rodziny.
 - Niepozostawiania loginu i hasła dostępu w miejscach widocznych dla innych osób.
 - Używania przekazanych urządzeń mobilnych jedynie w celach służbowych.
 - Nieudostępniania osobom nieuprawnionym programów komputerowych zainstalowanych na urządzeniach mobilnych.
 - Nieużywania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna.
 - Nieinstalowania oprogramowania i aplikacji innych niż zatwierdzone przez Dział Informatyczny.
 - Nieinstalowania dodatkowych urządzeń (np. twardych dysków, pamięci).
 - Niepodłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego.
 - Nieinstalowania i nieużywania jakichkolwiek programów komputerowych na użytek prywatny.

Urząd Miejski w Toszku

- Wykonywania kopii zapasowych plików i programów, w których dokonywano zmian.
- Niekopiowania danych na nośniki informacji, ani też na inne systemy.
- Nieużywania nośników danych prywatnych, niewiadomego pochodzenia, czy też udostępnionych przez osoby postronne.
- Nieprzesyłania dokumentów i danych służbowych z wykorzystaniem prywatnego konta pocztowego.
- Nieotwierania załączników i wiadomości poczty elektronicznej od nieznanых nadawców.
- Zabezpieczania urządzeń mobilnych przed kradzieżą, zniszczeniem lub nieuprawnionym dostępem do nich.
- Niezwłocznego zgłaszania Inspektorowi Ochrony Danych Osobowych zagubienia, kradzieży, zniszczenia i wszelkich innych incydentów związanych z powierzonymi urządzeniami mobilnymi.
- Uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach – tzw. Polityka czystego ekranu.
- Wywołania blokowanego hasłem wygaszacza ekranu lub wylogowania się z systemu bądź z programu, przed każdorazowym czasowym odejściem od laptopa.
- Ochrony wyświetlanych danych osobowych na monitorze przed wglądem osób nieupoważnionych podczas pracy w miejscach publicznych i środkach transportu.
- Niekorzystania z ogólnodostępnych, otwartych sieci wi-fi.
- Powiadomienia Działu Informatycznego o próbach logowania się do systemu przez osoby nieupoważnione, jeśli system to zasygnalizuje.
- Stosowania zasad określonych w Polityce bezpieczeństwa danych osobowych (oraz Instrukcji zarządzania systemem informatycznym – jeśli taka istnieje).

INSTRUKCJA OBSŁUGI SERWEROWNI

Do pomieszczeń serwerowni dostęp mają jedynie upoważnione osoby.

1. W pomieszczeniu serwerowni odbywa się transmisja, przetwarzanie i archiwizacja danych.
2. W serwerowni znajdują się instalacje elektryczne wraz z okablowaniem szczegółowo opisanym w skrzynce po lewej stronie od wejścia do serwerowni z napisem „Rozdzielnia TK”.
3. Wszelkie czynności związane z obsługą i konserwacją instalacji elektrycznej mogą wykonywać osoby posiadające odpowiednie świadectwo kwalifikacyjne w zakresie eksploatacji oraz zapoznały się dokumentacją instalacji elektrycznej.
4. W serwerowni znajdują się serwery, urządzenie firewall Fortinet wraz z switchami, laptop do obsługi serwera, dysk QNAP oraz komputery służące do przechowywania archiwalnych danych.
5. Na serwerze głównym znajduje się system Windows 2008, na pozostałych komputerach/sprzętach znajdują się systemy od Windowsa XP do Windows 7.
6. **CZYNNOŚCI ZABRONIONE:**
 - 1) Używania otwartego ognia, palenia tytoniu oraz stosowania czynników mogących wywołać zapłon w pomieszczeniach serwerowni.
 - 2) Wstęp do pomieszczeń serwerowni osób nieupoważnionych.
 - 3) Eksploatowanie niesprawnych urządzeń oraz instalacji elektrycznej.
 - 4) W przypadku pożaru gaszenie urządzeń oraz instalacji elektrycznej wodą.
 - 5) Samodzielne naprawy urządzeń elektrycznych.
 - 6) Składowanie przedmiotów i materiałów w przejściach serwerowni.

Kierownik Referatu
Zamówień Fumelanych,
Rozwoju i Promocji Gminy
mgr Iwona Filip

Adwokat
INFORMATYK
mgr Piotr Kunc

Zastępca Burmistrza
mgr Piotr Kunc

7. POSTĘPOWANIE NA WYPADEK AWARII

- 1) W razie stwierdzenia nieprawidłowości w pracy urządzeń serwerowni należy bezzwłocznie powiadomić przełożonego i Administratora Systemu Informatycznego (ASI)
- 2) Nie należy samodzielnie wyłączać urządzeń.
- 3) W przypadku samoczynnego wyłączenia się urządzenia, jego ponowne załączenie może nastąpić po ustaleniu i usunięciu przyczyny tego faktu.
- 4) O wszelkich usterkach i nieprawidłowościach w pracy urządzenia należy powiadomić przełożonego oraz Administratora Systemu Informatycznego (ASI).

8. POSTANOWIENIA OGÓLNE:

- 1) W przypadku pożaru/akcji gaśniczej należy natychmiast opuścić pomieszczenie serwerowni i udać się do bezpiecznego miejsca lub miejsca zbiórki.
- 2) Jeżeli podczas pobytu w serwerowni zaniknie zasilanie w serwerowni należy natychmiast poinformować o tym fakcie przełożonego i Administratora Systemu Informatycznego (ASI).
- 3) W razie nieumyślnego naciśnięcia jakiegokolwiek przycisku na sprzęcie znajdującym się w pomieszczeniu serwerowni należy niezwłocznie o tym fakcie poinformować przełożonego oraz Administratora Systemu Informatycznego (ASI).
- 4) Sprzątanie pomieszczeń serwerowni może prowadzić upoważniony personel, odpowiednio przeszkolony.

**KAŻDY, KTO ZAUWAŻY POŻAR W POMIESZCZENIU
SERWEROWNI ZOBOWIĄZANY JEST DO
NATYCHMIASTOWEGO ZAALARMOWANIA POZOSTAŁYCH
PRACOWNIKÓW OKRZYKIEM**

"POŻAR - PALI SIĘ".

**NALEŻY URUCHOMIĆ NAJBLIŻSZE URZĄDZENIE
OSTRZEGAWCZE PRZED POŻAREM.**

POWIADOMIĆ PRZEŁOŻONEGO ORAZ STRAŻ POŻARNĄ.

WYKAZ OSÓB UPOWAŻNIONYCH DO PRZEBYWANIA W POMIESZCZENIU SERWEROWNI

1. Burmistrz Toszka – Grzegorz Kupczyk

.....
Podpis

2. Główny Specjalista – Andrzej Pruski

.....
Podpis

3. Informatyk – Szymon Rabiza

.....
Podpis

Osoby wymienione powyżej lub osoby posiadające pisemną zgodę ADO
są upoważnione do dostępu do pomieszczenia serwerowni.

.....
Data

.....
Podpis ADO

REJESTR WEJŚĆ / WYJŚĆ Z SERWEROWNI

[illegible]

SPOSÓB ZDAWANIA I ODBIERANIA KLUCZY DO SERWEROWNI

1. Klucze do serwerowni przechowywane są w zabezpieczonej szafce w pokoju nr. 26.
2. Osobą odpowiedzialną za klucze jest Informatyk Urzędu Miejskiego w Toszku.
3. Klucze do serwerowni wydawane są przez Informatyka za potwierdzeniem. Klucze te pozostają pod osobistym nadzorem osób upoważnionych. Wydający klucze ma obowiązek weryfikacji tożsamości pobierającego z Wykazem osób upoważnionych do przebywania w pomieszczeniu serwerowni.
4. Pracownicy upoważnieni zobowiązani są do odnotowania pobrania i zdania kluczy.
5. Rejestr osób pobierających i zdających klucze znajduje się w pokoju nr. 26
6. Klucze do pokoju nr. 26 znajdują się w zabezpieczonym sejfie na klucze w pokoju nr. 19
7. Tylko osoby upoważnione do przebywania w serwerowni lub osoby posiadające pisemną zgodę ADO mogą otrzymać klucze do serwerowni.

INFORMATYK
Rabiza
Szymon Rabiza

REJESTR OSÓB POBIERAJĄCYH I ZDAJĄCYCH KLUCZE DO SERWEROWNI

DATA POBRANIA KLUCZY	DATA ZDANIA KLUCZY	PODPIS OSOBY POBIERAJĄCEJ KLUCZE	PODPIS OSOBY POTWIERDZAJĄCEJ ZDANIE KLUCZY