Zarządzenie Nr 370

Prezydenta Miasta Piotrkowa Trybunalskiego

z dnia 27 września 2019 roku

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemami Informatycznymi w Urzędzie Miasta Piotrkowa Trybunalskiego

Na podstawie art. 31, art. 33 ust. 1, 3 i 5 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. 2019 poz. 506 ze zm.), ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000 ze zm.) oraz 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.2016.119.1) **z a r z ą d z a m**, co następuje:

§ 1.

W celu zapewnienia ochrony danych, w tym danych osobowych w Urzędzie Miasta Piotrkowa Trybunalskiego wprowadzam:

1. **Politykę Bezpieczeństwa Informacji w Urzędzie Miasta Piotrkowa Trybunalskiego**, w brzmieniu określonym w załączniku Nr 1 do niniejszego zarządzenia.
2. **Instrukcję Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych w Urzędzie Miasta Piotrkowa Trybunalskiego**, w brzmieniu określonym w załączniku Nr 2 do niniejszego zarządzenia.

§ 2.

Zobowiązuję wszystkich pracowników Urzędu Miasta Piotrkowa Trybunalskiego do przestrzegania postanowień zawartych w **Polityce Bezpieczeństwa Informacji** oraz **Instrukcji Zarządzania Systemami Informatycznymi**, kierowników komórek organizacyjnych czynię zaś odpowiedzialnymi za sprawowanie nadzoru nad ich przestrzeganiem przez podległych pracowników.

§ 3.

Uchylam Zarządzenie Nr 399 Prezydenta Miasta Piotrkowa Trybunalskiego z dnia 20 września 2013 r.

§ 4.

Wykonanie Zarządzenia powierzam Kierownikowi Referatu Zarządzania Dokumentacją i Bezpieczeństwa Informacji oraz Kierownikowi Referatu Informatyki.

§ 5.

Nadzór nad wykonaniem Zarządzenia powierzam Sekretarzowi Miasta.

§ 6.

Zarządzenie wchodzi w życie z dniem podpisania.

Z up. PREZYDENTA MIASTA

Andrzej Kacperek

WICEPREZYDENT MIASTA

Załącznik nr 1 do Zarządzenia Nr 370
Prezydenta Miasta Piotrkowa Trybunalskiego
z dnia 27 września 2019 roku

POLITYKA BEZPIECZEŃSTWA INFORMACJI
W Urzędzie Miasta Piotrkowa Trybunalskiego

1. Kierownictwo Urzędu Miasta świadome wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających Urzędowi Miasta swoje dane osobowe do właściwej i skutecznej ochrony tych danych zapewnia:
   1) podejmowanie wszystkich działań z zakresu bezpieczeństwa informacji w szczególności danych osobowych niezbędnych dla ochrony praw osób fizycznych,
   2) stałe podnoszenie świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Urzędzie Miasta Piotrkowa Trybunalskiego w zakresie zapewnienia bezpieczeństwa tych danych,
   3) podejmowanie w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.
2. Kierownictwo Urzędu Miasta świadome, jak ważna jest ochrona danych osobowych, wdrożyło, utrzymuje i stale doskonali Zintegrowany System Zarządzania Jakością i Bezpieczeństwa Informacji zgodny z międzynarodowymi standardami norm ISO, w szczególności zaś spełnia wymagania normy ISO/IEC 27001:2005.
   Zgodnie z wymogami tej normy Urząd Miasta jest corocznie audytowany pod kątem utrzymania i rozwijania ochrony przetwarzanych w Urzędzie Miasta informacji, zwłaszcza danych osobowych. Zasady funkcjonowania ochrony informacji i danych osobowych zawarte są w Księdze Jakości i Bezpieczeństwa Informacji, a dla stosowania tych zasad wdrożono 10 polityk bezpieczeństwa informacji:
   - Politykę szacowania ryzyka
   - Politykę tworzenia kopii zapasowych i archiwizacji informacji
   - Politykę postępowania ze sprzętem i nośnikami danych
   - Politykę kontroli dostępu do systemu
   - Politykę czystego biurka i czystego pulpitu
   - Politykę zarządzania incydentami i słabościami systemu związanymi z bezpieczeństwem informacji
   - Politykę dostępu do pomieszczeń w strefach bezpieczeństwa
   - Politykę kontroli oprogramowania
   - Politykę zarządzania zabezpieczeniami kryptograficznymi
   - Politykę ciągłości działania.

Księga Jakości i Bezpieczeństwa Informacji oraz polityki bezpieczeństwa dostępne są dla pracowników Urzędu, w sieci wewnętrznej, na stronie ISON (www.iso.piotrkow.pl).

SPIS TREŚCI

Rozdział I

Postanowienia ogólne

§ 1

Podstawa prawna

1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2019.700 ze zm.);
2. Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U.2018.1000 ze zm.);
3. Ustawa z dnia 14 grudnia 2018r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U.2019.125 ze zm.);
4. Rozporządzenie 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.2016.119.1);
5. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017.2247 ze zm.).

§ 2

1. Polityka Bezpieczeństwa Informacji w Urzędzie Miasta Piotrkowa Trybunalskiego (zwana dalej Polityką Bezpieczeństwa) jest wewnętrznym dokumentem regulującym zasady bezpieczeństwa informacji w szczególności przetwarzania i ochrony danych osobowych w Urzędzie Miasta Piotrkowa Trybunalskiego (zwanego dalej Urzędem).
2. Polityka Bezpieczeństwa w zakresie ochrony danych osobowych w Urzędzie odnosi się do danych osobowych przetwarzanych w zbiorach danych:

1) tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych,
2) informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.

§ 3

Słownik skrótów i pojęć stosowanych w Polityce Bezpieczeństwa:

1. **ADO** - Administrator Danych Osobowych - należy przez to rozumieć Prezydenta Miasta Piotrkowa Trybunalskiego.
2. **ASI** – Administrator Systemów Informatycznych – należy przez to rozumieć Kierownika Referatu Informatyki odpowiedzialnego za prawidłowe funkcjonowanie Systemu oraz bezpieczeństwo przetwarzanych danych pod kątem teleinformatycznym.
3. **Baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe.
4. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
5. **Działanie korygujące** - działanie przeprowadzane w celu wyeliminowania przyczyny wykrytej niezgodności / incydentu lub innej niepożądanej sytuacji.
6. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
7. **Incydent** - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania systemu informatycznego i zagrażają bezpieczeństwu informacji, naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
8. **IOD** - Inspektor Ochrony Danych - pracownik Urzędu Miasta wspierający Administratora Danych Osobowych w realizacji obowiązków dotyczących ochrony danych osobowych.
9. **Kierownik DBI** – Kierownik Referatu Zarządzania Dokumentacją i Bezpieczeństwa Informacji, prowadzący postępowania wyjaśniające w przypadku stwierdzenia wystąpienia zagrożenia bezpieczeństwa informacji bądź incydentu.
10. **Korekcja** - działanie w celu wyeliminowania wykrytej niezgodności lub incydentu.

11. **Kontrola (Audyt)** - systematyczny, niezależny i udokumentowany proces oceny skuteczności systemu ochrony danych osobowych, na podstawie określonych kryteriów, wymagań polityk i procedur.

12. **Login** – (Identyfikator Użytkownika systemu) ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

13. **Niezgodność** - niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe.

14. **Nośniki danych** –płyty CD lub DVD, pamięć Flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/materiały służące do przechowywania plików z danymi.

15. **Odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią z wyłączeniem organów publicznych które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego. Przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

16. **Osoba upoważniona** - pracownik Urzędu Miasta posiadający upoważnienie do przetwarzania danych osobowych udzielone przez ADO lub przez osobę wyznaczoną, uprawnioną.

17. **Podatność** - luka (słabość systemu), która może być wykorzystana przez co najmniej jedno zagrożenie, rozumiane jako potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę dla Urzędu.

18. **Pracownik** – osoba fizyczna:
    a) świadcząca pracę na podstawie stosunku pracy, powołania, lub stosunku cywilnoprawnego,
    b) wykonująca zadania wyłącznie osobiście, w ramach prowadzonej działalności gospodarczej, powierzone jej na podstawie umowy cywilnoprawnej,
    c) współpracująca w rozumieniu ustawy z dnia 13 października 1998 roku o systemie ubezpieczeń społecznych (tekst jednolity Dz.U.2019.300 ze zm.).

19. **Profilowanie** – automatyczny proces przetwarzania danych osobowych, dopuszczalny pod warunkiem spełnienia przesłanek określonych przepisami prawa

20. **Przetwarzane danych** – wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych.

21. **RODO** - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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).

22. **Serwisant** – firma lub pracownik firmy zajmujący się instalacją, naprawą oraz konserwacją sprzętu komputerowego.

23. **Sieć publiczna** – sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych.

24. **Słabość systemu** - zdarzenie, stan rzeczy zwiększający ryzyko wystąpienia incydentu.

25. **System EZD** – system elektronicznego zarządzania dokumentacją stosowany w Urzędzie Miasta Piotrkowa Trybunalskiego.

26. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.

27. **System tradycyjny** - zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze.

28. **Teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.

29. **UODO** – Urząd Ochrony Danych Osobowych.

30. **Usuwanie danych** – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą.

31. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

32. **Użytkownik systemu** - osoba posiadająca indywidualny login oraz hasło służące do jego identyfikacji w celu umożliwienia dostępu do systemu informatycznego oraz korzystania z jego zasobów. Użytkownikiem systemu może być pracownik Urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w Urzędzie lub wolontariusz.

33. **Zabezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

34. **Zagrożenie** - potencjalna możliwość wystąpienia niepożądanego incydentu, którego skutkiem może być szkoda dla Urzędu.

35. **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

36. **Zdarzenie** - błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z zagrożeniem bezpieczeństwa danych.

§ 4

Klasyfikacja informacji przetwarzanych w Urzędzie:

1. **Informacje jawne** – ogólnodostępne informacje, nie objęte ochroną danych osobowych, których ujawnienie lub utrata nie spowoduje przerwy w działalności Urzędu Miasta oraz roszczeń stron trzecich;
2. **Informacje wrażliwe**:
   1) dane osobowe, podlegające ochronie prawnej,
   2) informacje zawierające dane chronione przez Urząd nie podlegające publikacji, których ujawnienie bądź utrata może spowodować straty bądź roszczenia stron trzecich.
3. **Informacje niejawne** o klauzuli poufne i zastrzeżone określone ustawą o ochronie informacji niejawnych.

§ 5

1. Polityka Bezpieczeństwa określa:
   1) granice dopuszczalnego zachowania Użytkowników systemu oraz wskazuje konsekwencje w stosunku do osób naruszających przepisy ustawy o ochronie danych osobowych,
   2) prawa i obowiązki Użytkowników systemu w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych przetwarzanych w tym systemie,
   3) sposób przetwarzania danych osobowych oraz środki organizacyjne i techniczne zapewniające ochronę tych danych,
   4) podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
   5) wymagania w zakresie odnotowywania udostępniania i bezpieczeństwa przetwarzania danych osobowych,
   6) instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych,
   7) sposób przepływu informacji pomiędzy poszczególnymi systemami,
   8) środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   1) **poufność danych** – rozumianą jako właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobom,
   2) **integralność danych** – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   3) **rozliczalność danych** - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
   4) **integralność systemu** - rozumianą jako nienaruszalność systemu, niemożność

jakiejkolwiek manipulacji zamierzonej, jak i przypadkowej,

5) **dostępność informacji** - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,

6) **zarządzanie ryzykiem** - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa informacji.

3. Polityka Bezpieczeństwa dostępna jest w wewnętrznej sieci Urzędu na stronie ISON.

4. Każdy pracownik Urzędu zobowiązany jest do zapoznania się z treścią niniejszej Polityki Bezpieczeństwa i przestrzegania jej postanowień.

Rozdział II

Zasady ogólne przetwarzania danych osobowych. Powierzenie. Udostępnianie. Zabezpieczenia. Odpowiedzialność. Obowiązek informacyjny

Zasady ogólne przetwarzania danych osobowych

§ 6

1. Dane osobowe w Urzędzie przetwarzane są w celu zabezpieczenia prawidłowej realizacji zadań wynikających z ustawy z dnia 8 marca 1990 roku o samorządzie gminnym oraz ustawy z dnia 5 czerwca 1998r. o samorządzie powiatowym.

   W szczególności dane osobowe przetwarza się w celu:

   1) realizacji celów strategicznych i operacyjnych Miasta wynikających ze Strategii Rozwoju Miasta,

   2) zapewnienia prawidłowej, zgodnej z prawem i celami Urzędu polityki kadrowej,

   3) realizacji innych, prawnie uzasadnionych celów ADO, z poszanowaniem praw i wolności osób powierzających Urzędowi swoje dane.

2. Zakres danych osobowych przetwarzanych przez jednego Użytkownika systemu nie może być szerszy, niż powierzony do przetwarzania w związku z wykonywanymi przez niego obowiązkami.

3. Po wygaśnięciu podstawy przetwarzania, dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.

§ 7

Obszarem przetwarzania danych osobowych są wydzielone pomieszczenia lub części pomieszczeń w siedzibach Urzędu.

§ 8

Wszystkie osoby, które przetwarzają dane osobowe w obszarze wymienionym w § 7, muszą posiadać pisemne upoważnienie dopuszczające do przetwarzania danych nadane przez ADO oraz podpisać oświadczenie o zachowaniu poufności tych danych. (*Wzór upoważnienia oraz oświadczenia o zachowaniu poufności stanowi załącznik nr 3 do niniejszej Polityki*).

§ 9

1. Upoważnienia dopuszczające do przetwarzania danych osobowych wydawane są zgodnie z właściwą procedurą określoną w niniejszej Polityce Bezpieczeństwa oraz w Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych w Urzędzie Miasta.
2. Upoważnienia, o których mowa w ust. 1, ważne są do dnia odwołania lub do chwili ustania zatrudnienia upoważnionego pracownika.

§ 10

1. W przypadku zaistnienia konieczności profilowania ADO obowiązkowo wdraża środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą.
2. O profilowaniu należy informować osobę, której ono dotyczy na etapie zbierania danych, a także na każdy wniosek osoby, której dane dotyczą.
3. Każda osoba, której dane dotyczą, ma prawo wyrażenia sprzeciwu na profilowanie przez Urząd jej danych osobowych, jeżeli uzna, że narusza to jej prawa i wolności.

§ 11

<u>Powierzenie przetwarzania danych osobowych</u>

1. Do przetwarzania powierzonych danych osobowych mogą być dopuszczeni jedynie pracownicy Urzędu oraz pracownicy podmiotów (podmiotów przetwarzających) świadczących usługi na jego rzecz w związku z realizacją celów i zadań administratora.
2. Powierzenie przetwarzania danych osobowych następuje na podstawie umowy powierzenia przetwarzania danych osobowych lub innego aktu (instrumentu) prawnego, zawartej w formie pisemnej lub dopuszczalnej prawem formie elektronicznej w postaci oświadczenia złożonego za pośrednictwem prawnie dopuszczonych środków komunikacji elektronicznej lub zapisanego na elektronicznym nośniku informacji. *(Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik nr 6 do niniejszej Polityki)*.
3. Zgodnie z art. 28 RODO, umowa powierzenia danych osobowych powinna określać przedmiot i czas trwania przetwarzania, zakres, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, obowiązki i prawa stron umowy (administratora i procesora).
4. Zakres danych osobowych powierzanych powinien być adekwatny do celu powierzenia.

5. Administrator danych osobowych zobowiązany jest do dokumentowania powierzania tych danych w postaci wykazu podmiotów, którym powierzono dane osobowe, za każdym razem, gdy takie powierzenie nastąpi *(wzór wykazu podmiotów, którym powierzono przetwarzanie danych stanowi załącznik nr 5 do niniejszej Polityki).*
6. W przypadku, w którym podmiot określony w umowie powierzenia danych osobowych, w zakresie realizacji swoich usług korzysta z pomocy innych podmiotów (podpowierzenie danych), wymagana jest szczegółowa lub ogólna zgoda Urzędu na przekazanie powierzonych danych, wyrażona w formie pisemnej lub równoważnej jej formie elektronicznej.

§ 12

Udostępnianie danych osobowych

1. Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie w sytuacji, w której administrator danych udostępniający dane oraz administrator danych pozyskujący dane drogą udostępnienia posiadają odpowiednią podstawę prawną w sprawie ww. czynności.
2. Administrator Danych Osobowych może odmówić udostępnienia danych osobowych w sytuacji, w której spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób oraz w sytuacji, w której dane osobowe nie mają istotnego związku ze wskazanymi motywami działania wnioskującego o udostępnienie danych.
3. W przypadku konieczności udostępniania dokumentów i danych w nich zawartych, wśród których znajdują się dane osobowe podlegające ochronie prawnej, należy bezwzględnie dokonać anonimizacji tych danych.
4. W przypadku, gdy dane osobowe osoby, od której zostały zebrane, są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy o ochronie danych osobowych lub są zbędne do realizacji celu, dla którego zostały zebrane, ADO lub osoba przez niego upoważniona jest zobowiązana do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

§ 13

Zabezpieczenia danych osobowych

W celu zapewnienia należytej ochrony przetwarzania danych osobowych, w Urzędzie zastosowano środki zabezpieczające powierzone zbiory danych w postaci zabezpieczeń technicznych i organizacyjnych.

I. Zabezpieczenia techniczne

1. Dokumenty zawierające dane osobowe w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w pomieszczeniach zabezpieczonych drzwiami zamykanymi na klucz w szafach zamykanych na klucz.

2. Obszary, w których przetwarzane są dane osobowe wyposażone są w przeciwwłamaniowy system alarmowy.
3. Obszary, w których przetwarzane są dane osobowe zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy.
4. Dostęp do obszarów, w których przetwarzane są dane osobowe kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych.
5. W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenia dokonuje się poprzez pocięcie w niszczarce.
6. Zastosowano urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.
7. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem loginu oraz hasła.
8. Zabrania się przekazywania osobom trzecim loginu i hasła użytkownika systemu nieobecnego na stanowisku pracy. W uzasadnionych przypadkach kierownik komórki lub osoba upoważniona wnioskuje do ASI celem uzyskania dostępu. Po powrocie nieobecny pracownik otrzymuje nowe indywidualne hasło dostępu.
9. O każdym zdarzeniu opisanym w ust. 8 ASI informuje IOD.
10. Dla potrzeb ochrony danych osobowych przetwarzanych w edytorach tekstu (Ms Word), arkuszach kalkulacyjnych (Ms Excel) lub programach równorzędnych (np. Open Office) i innych programach do tworzenia baz danych oraz w systemach informatycznych stosowanych w Urzędzie, zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie itp.
11. Do ochrony dostępu do sieci komputerowej użyto odpowiednich i rekomendowanych systemów Firewall.
12. Zastosowany system informatyczny umożliwia rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
13. Zastosowany system informatyczny umożliwia określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego w tym systemie zbioru danych osobowych.
14. Stosowany system informatyczny posiada mechanizm wymuszający okresową zmianę haseł dostępu.
15. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika systemu.

II. Zabezpieczenia organizacyjne

1. Opracowano i wdrożono *Politykę bezpieczeństwa* oraz *Instrukcję zarządzania systemami informatycznymi służącym do przetwarzania danych w* Urzędzie.

2. Wyznaczono Inspektora Ochrony Danych, który w imieniu ADO sprawuje nadzór nad przetwarzaniem danych osobowych.
3. Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie, o którym mowa w § 8 niniejszej Polityki Bezpieczeństwa i podpisały oświadczenie o zachowaniu poufności.
4. Prowadzone są wykazy osób i podmiotów, o których mowa w § 17 ust. 3 niniejszej Polityki Bezpieczeństwa.
5. Wszystkie osoby wykonujące czynności związane z przetwarzaniem danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
6. Wszyscy Użytkownicy systemu zostali przeszkoleni w zakresie zabezpieczeń tego systemu.
7. Urząd organizuje pracownikom cykliczne szkolenia wewnętrzne z zakresu ochrony danych osobowych.
8. Wszystkie osoby wykonujące czynności związane z przetwarzaniem danych osobowych obowiązane zostały do zachowania ich w tajemnicy, zgodnie z postanowieniami § 8 niniejszego dokumentu.
9. Wykonane kopie zapasowe zbiorów danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

§ 14

Odpowiedzialność

1. Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z ustawy o ochronie danych osobowych oraz postanowień RODO.
2. Za nieprzestrzeganie zasad uważa się w szczególności:
    1) przetwarzanie danych osobowych, do których nie jest się upoważnionym,
    2) przetwarzanie danych, których przetwarzanie jest zabronione,
    3) przetwarzanie danych niezgodne z celem utworzenia zbioru danych osobowych,
    4) udostępnianie lub umożliwianie dostępu do danych osobowych osobom nieupoważnionym,
    5) uniemożliwianie osobie, której dane dotyczą, korzystanie z przysługujących jej praw.
3. Kierownicy komórek organizacyjnych zobowiązani są do zgłaszania i aktualizacji wszystkich zbiorów danych osobowych, które przetwarzane są w podległej komórce organizacyjnej do IOD.
4. Kierownicy komórek organizacyjnych zobowiązani są do niezwłocznego powiadomienia IOD o wszelkich incydentach naruszeń ochrony danych osobowych w Urzędzie.

5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Polityki Bezpieczeństwa stanowią naruszenie obowiązków pracowniczych i skutkować będą odpowiedzialnością wynikającą z kodeksu pracy.

§ 15

Obowiązek informacyjny

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, ADO jest obowiązany podać jej informacje, o których mowa w art. 13 RODO.
2. W przypadku pozyskania danych osobowych w sposób inny niż od osoby, której dane dotyczą, ADO podaje osobie, której dane dotyczą informacje, o których mowa w art. 14 RODO.

Rozdział III

Inspektor Ochrony Danych

§ 16

1. Inspektora Ochrony Danych (IOD) w Urzędzie wyznacza, w drodze odrębnego zarządzenia, Prezydent Miasta.
2. ADO zapewnia aby IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych w Urzędzie. Wspiera IOD w wypełnianiu przez niego zadań, zapewniając zasoby niezbędne do ich wykonania oraz dostęp do danych osobowych i operacji przetwarzania.

§ 17

1. IOD wykonuje zadania określone w art. 39 RODO tj.:
   1) informuje administratora, podmioty przetwarzające oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich wynikających z RODO oraz innych przepisów krajowych i unijnych dotyczących ochrony danych osobowych, a także doradza im w tym zakresie,
   2) monitoruje przestrzeganie rozporządzenia RODO oraz innych przepisów krajowych i unijnych dotyczących ochrony danych osobowych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenie personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
   3) udziela na żądanie ADO zaleceń co do oceny skutków dla ochrony danych oraz monitoruje ich wykonania zgodnie z art. 35 RODO,

4) współpracuje z organem nadzorczym,

5) pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem na zasadach określonych w RODO.

2. IOD prowadzi rejestr czynności przetwarzania *(wzór rejestru stanowi załącznik nr 1 do Polityki Bezpieczeństwa)* oraz rejestr kategorii czynności przetwarzania w Urzędzie Miasta Piotrkowa Trybunalskiego *(wzór rejestru stanowi załącznik nr 2 do Polityki Bezpieczeństwa).*

3. W ramach nadzoru nad przetwarzaniem danych, IOD sprawdza w szczególności:

   1) podstawę przetwarzania,

   2) cele przetwarzania,

   3) zakres przetwarzania,

   4) czas przetwarzania,

   5) sposoby zabezpieczenia danych osobowych,

   ponadto zobowiązany jest do przeprowadzania analizy ryzyk związanych z zagrożeniami związanymi z przetwarzaniem danych osobowych.

4. IOD prowadzi ponadto:

   1) wykaz osób, którym nadano upoważnienia do przetwarzania danych osobowych,

   2) wykaz obszarów, w których przetwarzane są dane osobowe,

   3) wykaz podmiotów, którym powierzono przetwarzanie danych osobowych *(wg wzoru stanowiącego załącznik nr 5 do Polityki Bezpieczeństwa*),

   4) wykaz udostępnień danych osobowych innym podmiotom *(wg wzoru stanowiącego załącznik nr 7 do Polityki Bezpieczeństwa*),

   5) rejestr naruszeń ochrony danych osobowych *(wg wzoru stanowiącego załącznik nr 8 do Polityki Bezpieczeństwa*).

Rozdział IV

Ogólne warunki korzystania z systemu informatycznego

§ 18

1. Korzystanie z funkcjonalności systemu informatycznego jest możliwe pod warunkiem uzyskania upoważnienia do przetwarzania danych na podstawie złożonego wniosku do IOD o nadanie/zmianę dostępu dla osoby uprawnionej.

2. Każdy Użytkownik systemu jest zobowiązany do zapoznania się i zaakceptowania zasad korzystania z systemu informatycznego.

§ 19

1. Zgodnie z postanowieniami niniejszej *Polityki Bezpieczeństwa*, zabrania się Użytkownikowi systemu podejmowania jakichkolwiek czynności mających na celu naruszenie bezpieczeństwa przetwarzanych danych, w tym prób przełamania zabezpieczeń systemu.
2. W celu zapobieżenia nieautoryzowanemu dostępowi do systemu informatycznego Użytkownik systemu nie może przechowywać danych służących do logowania do systemu w miejscach dostępnych dla innych osób oraz ujawniać danych służących do logowania innym osobom.

§ 20

Szczegółowe procedury korzystania oraz zasady konfiguracji sprzętu komputerowego Użytkownika systemu reguluje *Instrukcja zarządzania systemami informatycznymi służącym do przetwarzania danych w* Urzędzie Miasta.

Rozdział V

Postępowanie na wypadek zagrożenia bezpieczeństwa danych osobowych

§ 21

1. Do typowych **zagrożeń bezpieczeństwa informacji** należą w szczególności:
    1) próby naruszenia ochrony danych:
        a) z zewnątrz - włamania do systemu, podsłuch, kradzież danych, wandalizm,
        b) z wewnątrz - nieumyślna lub celowa modyfikacja danych, kradzież danych, wandalizm, bezprawne udostępnienie
    2) programy destrukcyjne: wirusy, konie trojańskie, makra, bomby logiczne,
    3) awarie sprzętu lub uszkodzenie oprogramowania,
    4) zabór sprzętu lub nośników z danymi,
    5) usiłowanie zakłócenia działania systemu informatycznego,
    6) inne skutkujące utratą danych, bądź wejściem w ich posiadanie osób nieuprawnionych.
2. Do typowych **incydentów bezpieczeństwa informacji** należą w szczególności:
    1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
    3) nieprzestrzeganie zasad ochrony bezpieczeństwa informacji przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),

4) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

5) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki użytkowników systemu, utrata/zagubienie danych),

6) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

3. Do typowych źródeł informacji o zagrożeniach, incydentach lub podatnościach (słabościach systemu) zalicza się:

1) zgłoszenia od Użytkowników systemu,

2) alarmy z systemów informatycznych,

3) analizę zagrożeń i incydentów przeprowadzona przez kierownika DBI,

4) wyniki audytów / kontroli.

§ 22

W przypadku stwierdzenia wystąpienia zagrożenia, Kierownik DBI prowadzi postępowanie wyjaśniające, w toku którego:

a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,

b) inicjuje ewentualne działania dyscyplinarne,

c) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,

d) dokumentuje prowadzone postępowania.

§ 23

W przypadku stwierdzenia incydentu (naruszenia) Kierownik DBI prowadzi postępowanie wyjaśniające, w toku którego:

a) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały i zabezpiecza ewentualne dowody oraz podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),

b) ustala osoby odpowiedzialne za naruszenie,

c) inicjuje działania dyscyplinarne, wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,

d) dokumentuje prowadzone postępowania.

§ 24

Kierownik DBI jest odpowiedzialny za analizę zagrożeń i incydentów bezpieczeństwa informacji oraz innych podatności (słabości systemu) w zakresie ochrony danych

osobowych. W razie stwierdzenia konieczności podjęcia działań korygujących lub zapobiegawczych, określa źródło ich powstania, zakres działań korygujących lub zapobiegawczych, termin realizacji oraz osobę odpowiedzialną.

§ 25

Kierownik DBI sprawuje nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych. Po przeprowadzeniu korekty lub działań korygujących, jest zobowiązany do oceny efektywności ich zastosowania i prowadzenia stosownej dokumentacji.

Rozdział VI

Postanowienia końcowe

§ 26

W sprawach nieuregulowanych niniejszą Polityką Bezpieczeństwa, znajdują zastosowanie przepisy ustawy o ochronie danych osobowych oraz RODO.

§ 27

Z dniem wejścia w życie niniejszej Polityki Bezpieczeństwa tracą moc upoważnienia do przetwarzania danych osobowych udzielone przed 23 sierpnia 2019 roku.

Załączniki:

Załącznik Nr 1 - Wzór rejestru czynności przetwarzania
Załącznik Nr 2 – Wzór rejestru kategorii czynności przetwarzania w Urzędzie Miasta Piotrkowa Trybunalskiego
Załącznik Nr 3 - Wzór upoważnienia dopuszczającego do przetwarzania danych osobowych wraz z oświadczeniem o zachowaniu poufności
Załącznik Nr 4 – Informacja dla pracowników Urzędu Miasta
Załącznik Nr 5 - Wykaz podmiotów, którym powierzono przetwarzanie danych osobowych
Załącznik Nr 6 – Wzór umowy powierzenia przetwarzania danych osobowych
Załącznik Nr 7 - Wykaz udostępnień danych osobowych innym podmiotom
Załącznik Nr 8 - Rejestr naruszeń ochrony danych osobowych
Załącznik Nr 9 – Protokół naruszenia ochrony danych osobowych
Załącznik Nr 10 – Wymagania w zakresie bezpieczeństwa informacji dla kontrahentów oraz podmiotów współpracujących z Urzędem Miasta Piotrkowa Trybunalskiego.

Z up. PREZYDENTA MIASTA
Andrzej Kacperek
WICEPREZYDENT MIASTA

Załącznik nr 2 do Zarządzenia Nr...370...
Prezydenta Miasta Piotrkowa Trybunalskiego
z dnia ...27 września... 2019 roku

INSTRUKCJA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH W URZĘDZIE MIASTA PIOTRKOWA TRYBUNALSKIEGO

I . Cel instrukcji

Celem Instrukcji jest określenie zasad zarządzania systemami informatycznymi stosowanymi w Urzędzie Miasta oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać wchodzące w jego skład urządzenia, odpowiednio do skali zagrożeń i kategorii danych objętych ochroną.
Stosowanie zasad określonych w niniejszej Instrukcji ma na celu zapewnienie prawidłowej ochrony informacji przetwarzanych przez URZĄD MIASTA PIOTRKOWA TRYBUNALSKIEGO w systemach informatycznych rozumiane jako ochronę informacji przed utratą poufności, dostępności i integralności.

II . Zakres stosowania

Instrukcję stosuje się do przetwarzania danych w systemach informatycznych. Instrukcję stosuje się również do przetwarzania danych zapisanych w postaci elektronicznej na zewnętrznych nośnikach informacji. Instrukcja zawiera specyfikację podstawowych środków technicznych ochrony danych oraz elementów zarządzania systemem informatycznym.

III . Definicje

Słownik skrótów i pojęć stosowanych w Instrukcji:

1. **ADO** - Administrator Danych Osobowych - należy przez to rozumieć Prezydenta Miasta Piotrkowa Trybunalskiego.
2. **ASI** – Administrator Systemów Informatycznych – należy przez to rozumieć Kierownika Referatu Informatyki odpowiedzialnego za prawidłowe funkcjonowanie Systemu oraz bezpieczeństwo przetwarzanych danych pod kątem teleinformatycznym.
3. **Administrator systemu** - informatyk zajmujący się zarządzaniem systemem informatycznym i odpowiadający za jego sprawne działanie. Uprawnienia Administratorowi systemu przydziela i cofa ASI
4. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

5. **IOD** - Inspektor Ochrony Danych - pracownik Urzędu Miasta wspierający Administratora Danych Osobowych w realizacji obowiązków dotyczących ochrony danych osobowych, wyznaczony w drodze odrębnego zarządzenia Prezydenta Miasta.
6. **Login** (Identyfikator Użytkownika systemu) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
7. **Osoba upoważniona** – pracownik Urzędu Miasta posiadający upoważnienie do przetwarzania danych osobowych udzielone przez ADO lub przez osobę wyznaczoną, uprawnioną.
8. **Przetwarzanie danych osobowych** - wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych.
9. **Sieć lokalna** – należy przez to rozumieć połączenie systemów informatycznych Urzędu Miasta wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci Telekomunikacyjnych.
10. **Sieć rozległa** – sieć publiczna w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. 2018.1954 ze zm.).
11. **System informatyczny** – należy przez to rozumieć zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
12. **Urząd** – należy przez to rozumieć Urząd Miasta Piotrkowa Trybunalskiego.
13. **Użytkownik systemu** - osoba posiadająca indywidualny login oraz hasło służące do jego identyfikacji w celu umożliwienia dostępu do systemu informatycznego oraz korzystania z jego zasobów. Użytkownikiem systemu może być pracownik Urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w Urzędzie lub wolontariusz.
14. **ZSZJiBI** - Zintegrowany System Zarządzania Jakością i Bezpieczeństwa Informacji, zgodny z normami ISO stosowanymi w Urzędzie Miasta.

IV . Zarządzanie bezpieczeństwem systemów

1. Podstawowe cele zabezpieczeń danych
   1.1 Podstawowym celem zabezpieczeń systemów informatycznych służących do przetwarzania danych jest zapewnienie jak najwyższego poziomu bezpieczeństwa.
   1.2 W celu zachowania odpowiedniego poziomu bezpieczeństwa przetwarzania danych, dostęp do systemu informatycznego przetwarzającego dane powinien być możliwy

wyłącznie po podaniu loginu odrębnego dla każdego użytkownika systemu i poufnego hasła lub innego elementu uwierzytelniającego.

2. Podstawowe zasady zabezpieczeń systemów
   2.1. Należy zapewnić poufność, integralność i rozliczalność systemów informatycznych służących do przetwarzania danych.
   2.2. Należy zapewnić aby użytkownicy systemów służących do przetwarzania danych nie posiadali wyższych poziomów uprawnień w tych systemach niż wymagane do wykonywania powierzonych obowiązków (dostępność).
   2.3. Należy zapewnić aby wszelkie działania użytkowników systemów zapewniały rozliczalność tych działań.
3. Prawidłowy poziom zabezpieczeń danych w systemach informatycznych zostaje zapewniony poprzez przestrzeganie polityk bezpieczeństwa stosowanych w Urzędzie.

V . Procedury nadawania i zmiany uprawnień do przetwarzania danych

1. Każdy użytkownik systemu przed przystąpieniem do korzystania z systemów informatycznych stosowanych w Urzędzie ma obowiązek zapoznać się z:
   1.1. aktualnymi przepisami prawa dotyczącymi bezpieczeństwa informacji i ochrony danych osobowych;
   1.2. Polityką Jakości i Bezpieczeństwa Informacji oraz dokumentacją Zintegrowanego Systemu Zarządzania Jakością i Bezpieczeństwa Informacji w Urzędzie Miasta Piotrkowa Trybunalskiego;
   1.3. niniejszą instrukcją.
2. Zapoznanie się z przepisami wymienionymi w ust. 1 pracownik potwierdza własnoręcznym podpisem na oświadczeniu o zachowaniu poufności stanowiącym integralną część upoważnienia do przetwarzania danych osobowych.
3. Administratorzy systemu przyznają uprawnienia w zakresie dostępu do systemów informatycznych na podstawie wniosku bezpośredniego przełożonego pracownika lub Sekretarza Miasta, określającego zakres uprawnień pracownika zgodnie z polityką kontroli dostępu do systemu.
4. Wygaśnięcie uprawnień do systemu, następuje na wniosek bezpośredniego przełożonego pracownika lub Sekretarza Miasta zgodnie z polityką kontroli dostępu do systemu.

5. Wyłączenie dostępu do systemów informatycznych następuje z chwilą wygaśnięcia uprawnień dostępu do systemów informatycznych.
6. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu dla każdego użytkownika systemu unikalnego loginu, hasła oraz zakresu dostępnych danych i operacji.
7. Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony.
8. Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego loginu i hasła dostępu.
9. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą, jako naruszenie podstawowych obowiązków pracowniczych.
10. Pracownik zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w tajemnicy.
11. W systemie informatycznym stosuje się uwierzytelnianie dwustopniowe: na poziomie dostępu do sieci lokalnej oraz dostępu do aplikacji.
12. Kierownicy komórek organizacyjnych zobowiązani są informować Kierownika Referatu Informatyki o każdej zmianie dotyczącej podległych pracowników mającej wpływ na zakres posiadanych uprawnień w systemie informatycznym.
13. Login osoby, która utraciła uprawnienia do dostępu do danych osobowych należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jej hasło.

VI . Zasady posługiwania się hasłami

1. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu loginu i hasła.
2. Hasło powinno być zmieniane przez użytkownika systemu, co najmniej raz w miesiącu. W przypadku gdy funkcjonalność danego systemu nie zapewnia automatycznego wymuszania zmiany haseł, należy zobligować pracowników do samodzielnej zmiany haseł, zgodnie z zasadami przyjętymi dla danego systemu informatycznego.
3. Login użytkownika systemu nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie powinien być przydzielany innej osobie.
4. Pracownicy są odpowiedzialni za zachowanie poufności swoich haseł.
5. Hasła użytkownika systemu utrzymuje się w tajemnicy również po upływie ich ważności.

6. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
7. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej jego zmiany.
8. Przy wyborze hasła obowiązują następujące zasady:

8.1 minimalna długość hasła - 8 znaków;

8.2 nie należy stosować:

8.2.1 swojej nazwy użytkownika systemu w jakiejkolwiek formie (pisanej dużymi literami, w odwrotnym porządku, dublując każdą literę, itp.),

8.2.2 swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie,

8.2.3 imion (w szczególności imion osób z najbliższej rodziny),

8.2.4 ogólnie dostępnych informacji o użytkowniku systemu takich jak: numer telefonu, numer rejestracyjny samochodu, jego marka, numer dowodu osobistego, nazwa ulicy, na której mieszka lub pracuje, itp.,

8.2.5 wyrazów słownikowych,

8.2.6 przewidywalnych sekwencji znaków z klawiatury np.: QWERTY", "12345678", itp.,

8.2.7 loginu użytkownika systemu;

8.3 należy stosować:

8.3.1. hasła zawierające kombinacje liter i cyfr,

8.3.2. hasła zawierające znaki specjalne: znaki interpunkcyjne, nawiasy, symbole @, #, &, itp., o ile system informatyczny na to pozwala,

8.3.3. hasła, które można zapamiętać bez zapisywania,

8.3.4. hasła łatwe i szybkie do wprowadzenia, po to by trudniej było podejrzeć je osobom trzecim.

9. Zmiany hasła nie wolno zlecać innym osobom.
10. W systemach, które umożliwiają opcję zapamiętania nazw użytkownika systemu lub jego hasła nie należy korzystać z tego ułatwienia.
11. Użytkownicy systemu powinni być świadomi swojej odpowiedzialności za utrzymanie skutecznej kontroli dostępu, szczególnie w odniesieniu do haseł i zabezpieczenia swojego sprzętu.
12. Hasło użytkownika systemu o prawach administratora powinno znajdować się w zamykanej na klucz szafie metalowej, do której dostęp ma ASI.

VII . Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego loginu oraz hasła.
2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wylogowania z systemu (zablokowania dostępu), lub jeżeli taka możliwość nie istnieje wyjść z programu.
3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu.
4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i jeżeli jest to konieczne wylogować się z sieci komputerowej
5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.
6. W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest powiadomić o tym fakcie przełożonego, ASI bądź IOD.

VIII . Procedury tworzenia zabezpieczeń

1. Za systematyczne przygotowanie kopii bezpieczeństwa (dane, które mają służyć do odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia) odpowiada ASI.
2. Kopie bezpieczeństwa wykonywane są zgodnie z Polityką tworzenia kopii zapasowych i archiwizacji informacji ZSZJiBI (Pol_02) i przechowywane w dwóch różnych lokalizacjach.
3. Płyty CD-R/DVD-R przechowuje się w kasie pancernej w pokoju 105 w budynku Urzędu przy Pasażu Rudowskiego 10.
4. W przyjętym systemie archiwizacji za ochronę danych na dyskach lokalnych odpowiedzialny jest użytkownik systemu na danym stanowisku pracy.

IX . Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruki

1. Elektroniczne nośniki informacji:

1.1. Generalnie nie przewiduje się tworzenia nośników elektronicznych zawierających dane osobowe poza sytuacjami wystąpienia wyższej konieczności utworzenia takiego nośnika;

1.2. Sposób postępowania z nośnikami elektronicznymi zawierającymi dane osobowe określony jest w Polityce postępowania ze sprzętem i nośnikami danych ZSZJiBI (Pol_03);

1.3. Wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określonych w ZSZJiBI;

1.4. Po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji są przechowywane w zamykanych szafach biurowych lub kasetkach;

1.5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;

1.6. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej.

2. Kopie zapasowe:

2.1. Kopie zapasowe zbioru danych osobowych oraz oprogramowania i narzędzi programowych zastosowanych do przetwarzania danych są przechowywane w kasie pancernej w pokoju 105 w budynku Urzędu przy Pasażu Rudowskiego 10;

2.2. Dostęp do danych opisanych w ust. 2.1 ma ASI, IOD oraz upoważnieni pracownicy Referatu Informatyki.

3. Wydruki:

3.1. W przypadku konieczności przechowywania wydruków zawierających dane osobowe należy je przechowywać w miejscu uniemożliwiającym bezpośredni dostęp osobom niepowołanym;

3.2. Pomieszczenie, w którym przechowywane są wydruki robocze musi być należycie zabezpieczone po godzinach pracy;

3.3. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

X. Środki ochrony systemu przed złośliwym oprogramowaniem, w tym wirusami komputerowymi

1. Na każdym stanowisku komputerowym musi być zainstalowane oprogramowanie antywirusowe pracujące w trybie monitora.

2. Definicje wzorców wirusów powinny być aktualizowane przynajmniej raz w czasie dnia.
3. Zasady kontroli oprogramowania opisane są w Polityce ZSZJiBI (Pol_08).
4. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik systemu, który pobrał plik.
5. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
6. W przypadku wystąpienia alertów wirusowych (wykrycia wirusów komputerowych) postępuje się zgodnie z Polityką zarządzania incydentami i słabościami systemu związanymi z bezpieczeństwem informacji ZSZJiBI (Pol_06).

XI. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

1. Dane osobowe z eksploatowanych systemów mogą być udostępniane wyłącznie osobom upoważnionym.
2. Udostępnienie danych osobowych nie może być realizowane drogą telefoniczną ani pocztą elektroniczną.
3. Udostępnienie danych osobowych następuje po przedstawieniu wniosku wg wzoru określonego w obowiązujących przepisach prawa.
4. Pracownicy prowadzą rejestry udostępnionych danych osobowych zawierające, co najmniej: datę udostępnienia, podstawę, zakres udostępnionych informacji oraz osobę lub instytucję, dla której dane udostępniono.
5. Aplikacje wykorzystywane do obsługi baz danych osobowych powinny zapewniać odnotowanie informacji o udzielonych odbiorcom danych. Zakres informacji powinien obejmować, co najmniej: dane odbiorcy, datę wydania, zakres udostępnionych danych.

XII . Postępowanie w sytuacji naruszenia ochrony danych osobowych

1. Naruszenie systemu ochrony danych osobowych może zostać stwierdzone na podstawie oceny:
   1.1. stanu urządzeń technicznych;
   1.2. zawartości zbiorów danych osobowych;
   1.3. sposobu działania programu lub jakości komunikacji w sieci teleinformatycznej;

1.4. metod pracy (w tym obiegu dokumentów).

3. W przypadku stwierdzenia naruszenia ochrony danych osobowych należy bezzwłocznie:
   3.1. powiadomić bezpośredniego przełożonego, ASI, IOD bądź ADO;
   3.2. zablokować dostęp do systemu dla użytkowników systemu oraz osób nieupoważnionych;
   3.3. podjąć działania mające na celu zminimalizowanie lub całkowite wyeliminowanie powstałego zagrożenia - o ile czynności te nie spowodują przekroczenia uprawnień pracownika;
   3.4. zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia bezpieczeństwa systemu.
4. Bezpośredni przełożony pracownika po otrzymaniu powiadomienia o naruszeniu bezpieczeństwa danych osobowych jest zobowiązany niezwłocznie powiadomić ASI, IOD lub ADO chyba, że zrobił to uprzednio pracownik, który stwierdził naruszenie.
5. Na stanowisku, na którym stwierdzono naruszenie zabezpieczenia danych, IOD i bezpośredni przełożony pracownika przejmują nadzór nad pracą w systemie odsuwając jednocześnie od stanowiska pracownika, który dotychczas na nim pracował, aż do czasu wydania odmiennej decyzji.
6. IOD lub osoba przez niego wyznaczona podejmuje czynności wyjaśniające mające na celu ustalenie:
   6.1. przyczyn i okoliczności naruszenia bezpieczeństwa danych osobowych;
   6.2. osób winnych naruszenia bezpieczeństwa danych osobowych;
   6.3. skutków naruszenia.
7. IOD zobowiązany jest do powiadomienia o zaistniałej sytuacji ADO, który podejmuje decyzję o wykonaniu czynności zmierzających do przywrócenia poprawnej pracy systemu oraz o ponownym przystąpieniu do pracy w systemie.
8. IOD zobowiązany jest do sporządzenia pisemnego raportu na temat zaistniałej sytuacji, zawierającego, co najmniej:
   8.1. datę i miejsce wystąpienia naruszenia;
   8.2. zakres ujawnionych danych;
   8.3. przyczynę ujawnienia, osoby odpowiedzialne oraz stosowne dowody winy;
   8.4. sposób rozwiązania problemu;
   8.5. przyjęte rozwiązania mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
9. Raport IOD przekazuje ADO.

10. W przypadku następującego permanentnie naruszenia ochrony danych osobowych bezwzględnie należy:
    1.1 zabezpieczyć kopie archiwalne danych,
    1.2 cofnąć uprawnienia wszystkich użytkowników systemu posiadających dostęp do zagrożonej bazy danych osobowych.

XIII. Procedury wykonywania przeglądów i konserwacji systemu

1. Przeglądy i konserwacja urządzeń:
   1.1. Zasady postępowania opisane są w Polityce postępowania ze sprzętem i nośnikami danych ZSZJiBI (Pol_03).
2. Przegląd programów i narzędzi programowych:
   2.1. Konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów;
   2.2. Wszystkie logi opisujące pracę systemu, zameldowania i wymeldowania użytkowników systemu oraz rejestr z systemu śledzenia wykonywanych operacji jest trwale zapisane w bazie danych programu. Ponadto w Urzędzie wykorzystywany jest system monitorowania umożliwiający rozliczalność każdego użytkownika systemu.
3. Rejestracja działań konserwacyjnych, awarii oraz napraw:
   Zasady postepowania opisane są w Polityce postępowania ze sprzętem i nośnikami danych ZSZJiBI (Pol_03) oraz w Polityce zarządzania incydentami i słabościami systemu związanymi z bezpieczeństwem informacji ZSZJiBI (Pol_06).

XIV. Zarządzanie bezpieczeństwem sieci

1. ASI zobowiązany jest chronić system przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, tj.:
   - kontrolę przepływu informacji pomiędzy systemem informatycznym a siecią publiczną;
   - kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.

2. Wewnętrzna adresacja IP, konfiguracja oraz informacja o systemach powiązanych nie powinna być ujawniana osobom nieuprawnionym bez akceptacji ze strony uprawnionej do tego celu osoby.
3. Podłączanie do infrastruktury sieciowej nieautoryzowanych urządzeń takich jak modemy, urządzenia sieciowe, w tym urządzenia sieci bezprzewodowych jest zabronione.
4. Podłączanie we własnym zakresie stacji roboczych do publicznej sieci telekomunikacyjnej poprzez nieautoryzowane urządzenia sieciowe, będąc jednocześnie podłączonym do infrastruktury lokalnej LAN jest zabronione.
5. Użytkownikom systemu należy zapewnić dostęp tylko do tych usług infrastruktury teleinformatycznej (np. dostęp do Internetu, zdalny dostęp, poczta elektroniczna), do których zostali autoryzowani.
6. Osoby niebędące pracownikami nie powinny posiadać nieautoryzowanego i niekontrolowanego dostępu do infrastruktury teleinformatycznej.
7. Niezabezpieczone usługi infrastruktury teleinformatycznej, pozwalające przesyłać hasła w postaci niezabezpieczonej (np. telnet lub ftp) nie powinny być wykorzystywane i powinny być zablokowane.
8. Wykonywane połączenia do Internetu są monitorowane i rejestrowane.
9. Systemy monitorowania połączeń do Internetu powinny rejestrować źródłowy adres IP, datę i godzinę połączenia, wykorzystywany protokół, docelową witrynę lub urządzenie (adres IP) oraz nazwę użytkownika systemu nawiązującego połączenie.
10. Dostęp do Internetu powinien być zabezpieczony poprzez zastosowanie narzędzi służących do blokowania stron internetowych lub usług zawierających niepożądane treści lub zawartość (np. materiały o charakterze pornograficznym, nielegalnym, obraźliwym, szkodliwe oprogramowanie oraz usługi udostępniania plików).
11. Użytkownicy systemu powinni być uświadamiani o zagrożeniach występujących podczas korzystania z Internetu.
12. Użytkownicy nie powinny instalować żadnego oprogramowania ściągniętego z Internetu bez upewniania się czy został on ściągnięty z zaufanej strony oraz czy nie zagraża bezpieczeństwu systemów informatycznych.
13. Poczta elektroniczna nie może być wykorzystywana do przesyłania informacji zawierających treści obraźliwe, szkodliwe, nielegalne, pornograficzne, dotyczące przekonań politycznych i uprzedzeń rasowych.

14. Wykorzystywanie prywatnych skrzynek pocztowych znajdujących się poza domeną pocztową piotrkow.pl do przesyłania informacji służbowych jest niedozwolone chyba, że zastosowano właściwe zabezpieczenia uzgodnione wcześniej z IOD i ASI.
15. Przychodzące i wychodzące wiadomości poczty elektronicznej należy sprawdzać na wypadek występowania wirusów i kodów złośliwych a potencjalnie niebezpieczne załączniki należy blokować.
16. Wiadomości poczty elektronicznej otrzymane z nieznanych i podejrzanych źródeł nie powinny być otwierane i przekazywane dalej.
17. Wewnętrzne adresy poczty elektronicznej nie powinny być udostępniane i ujawniane osobom nieuprawnionym.
18. Wewnętrzna lista adresowa powinna być zabezpieczona przed nieautoryzowanym dostępem i modyfikacją.

XV. Postanowienia końcowe

1. W sprawach nieuregulowanych w Instrukcji mają zastosowanie przepisy ustawy z dnia 10 maja 2018 r., o ochronie danych osobowych (Dz.U. 2018 poz. 1000 ze zm.)
2. Użytkownicy systemu przy przetwarzaniu danych osobowych zobowiązani są do bezwzględnego stosowania postanowień zawartych w niniejszej Instrukcji.

Z up. PREZYDENTA MIASTA

Andrzej Kacperek
WICEPREZYDENT MIASTA

Załącznik nr 1 do Polityki Bezpieczeństwa Informacji

Wzór Rejestru Czynności Przetwarzania

NAZWA ZBIORU DANYCH OSOBOWYCH	ADMINISTRATOR DANYCH	INSPEKTOR OCHRONY DANYCH	PODMIOT, KTÓREMU POWIERZONO PRZETWARZANIE DANYCH OSOBOWYCH	PODSTAWA PRZETWARZANIA	CEL PRZETWARZANIA DANYCH W ZBIORZE

Załącznik nr 1 do Polityki Bezpieczeństwa Informacji

Wzór Rejestru Czynności Przetwarzania

NAZWA KOMÓRKI ORGANIZACYJNEJ URZĘDU MIASTA, W KTÓREJ ZBIÓR ISTNIEJE	OPIS KATEGORII OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE W ZBIORZE	KATEGORIE DANYCH OSOBOWYCH PRZETWARZANYCH W ZBIORZE	SPOSÓB ZBIERANIA DANYCH DO ZBIORU	SPOSÓB UDOSTĘPNIANIA DANYCH ZE ZBIORU	ODBIORCA DANYCH / KATEGORIA ODBIORCÓW, KTÓRYM DANE ZOSTAŁY LUB ZOSTANĄ UJAWNIONE

Załącznik nr 1 do Polityki Bezpieczeństwa Informacji

Wzór Rejestru Czynności Przetwarzania

KATEGORIE ODBIORCÓW Z PAŃSTWA TRZECIEGO (GDY MA TO ZASTOSOWANIE)	PLANOWANE TERMINY USUNIĘCIA POSZCZEGÓLNYCH KATEGORII DANYCH (JEŚLI JEST TO MOŻLIWE)	OGOLNY OPIS TECHNICZNYCH I ORGANIZACYJNYCH ŚRODKÓW BEZPIECZEŃSTWA (JEŚLI JEST TO MOŻLIWE)	UWAGI

Z up. PREZYDENTA MIASTA

Andrzej Kasperek

WICEPREZYDENT MIASTA

Załącznik Nr 2 do Polityki Bezpieczeństwa Informacji

WZÓR REJESTRU KATAEGORII CZYNNOŚCI PRZETWARZANIA W URZĘDZIE MIASTA PIOTRKOWA TRYBUNALSKIEGO

L.p.	Administrator powierzający przetwarzanie	Przedstawiciel Administratora (jeśli nie ma zastosowania wpisać nd.)	Inspektor ochrony danych Administratora	Kategorie przetwarzań w imieniu Administratora	Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej	Ogólny opis techniczynych i organizacyjnych środków bezpieczeństwa	data utworzenia wpisu

Z up. PREZYDENTA MIASTA

Andrzej Kacperek
WICEPREZYDENT MIASTA

Załącznik nr 3 do Polityki Bezpieczeństwa Informacji

..... Piotrków Trybunalski dn.,.....

(pieczęć Administratora Danych Osobowych)

U P O W A Ż N I E N I E Nr ...../20.... r

DOPUSZCZAJĄCE DO PRZETWARZANIA DANYCH OSOBOWYCH

Prezydent Miasta Piotrkowa Trybunalskiego – Administrator Danych Osobowych, działając na podstawie Art. 29 Rozporządzenia 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,

upoważnia do przetwarzania danych osobowych, w Urzędzie Miasta w Piotrkowie Trybunalskim

Pana/Panią

_____

(imię i nazwisko)

Stanowisko służbowe

w (nazwa komórki organizacyjnej)

w zakresie edycji/przeglądania: (programów oraz systemów komputerowych) oraz przetwarzania danych osobowych w zbiorach danych: (wymienić zbiory danych osobowych zgodnie z Rzeczowym Wykazem Akt)

_____

(imienna pieczęć i podpis Administratora Danych Osobowych)

Z up. PREZYDENTA MIASTA

Andrzej Kacperek

WICEPREZYDENT MIASTA

Imię i nazwisko
Stanowisko służbowe
Komórka organizacyjna

Oświadczenie

Oświadczam, że zostałem zapoznany z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych, w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) i zobowiązuję się do przestrzegania w/w przepisów oraz przetwarzania i ochrony danych osobowych zgodnie z tymi przepisami.

Ponadto oświadczam, że zobowiązuję się do zachowania w tajemnicy treści danych osobowych oraz sposobu ich zabezpieczania, do których posiadam dostęp na podstawie niniejszego upoważnienia dopuszczającego do przetwarzania danych osobowych wydanego przez Prezydenta Miasta Piotrkowa Trybunalskiego, także po wygaśnięciu otrzymanego upoważnienia.

Powyższe oświadczenie składam będąc świadomy, iż na podstawie art. 233 § 1 Kodeksu karnego za podanie nieprawdy lub zatajenie prawdy grozi kara pozbawienia wolności.

Piotrków Tryb. dnia:.....

.....
(podpis osoby zobowiązanej)

.....
Data i podpis osoby szkolącej

Z up. PREZYDENTA MIASTA
Andrzej Kasperek
WICEPREZYDENT MIASTA

Załącznik nr 4 do Polityki Bezpieczeństwa Informacji

INFORMACJA DLA PRACOWNIKÓW URZĘDU MIASTA

Mając na względzie dbałość o właściwe dysponowanie danymi osobowymi oraz mając na względzie rozpoczęcie obowiązywania przepisów Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 2019/679 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 (RODO) a w szczególności art. 13 RODO informujemy że:

W Urzędzie Miasta Piotrkowa Trybunalskiego zastosowany został system monitoringu z wykorzystaniem kamer przemysłowych obejmujący wizję i fonię, monitoring czasu pracy oraz monitoring wszelkich czynności wykonywanych na komputerze, ruchu internetowego oraz wydruków.

Informacje zgromadzone w wyniku działania monitoringu mają na celu wyłącznie zwiększenie bezpieczeństwa pracy oraz umożliwienie wykrywania zachowań szkodzących Urzędowi Miasta lub narażających go na straty i nie zostaną wykorzystane w żadnym innym celu.

Z up. PREZYDENTA MIASTA
Andrzej Kacperek
WICEPREZYDENT MIASTA

Załącznik nr 5 do Polityki Bezpieczeństwa Informacji

WYKAZ PODMIOTÓW KTÓRYM POWIERZONO PRZETWARZANIE DANYCH OSOBOWYCH

L.p.	Nazwa podmiotu, któremu powierzono dane	Data powierzenia	Cel powierzenia oraz numer umowy powierzenia	Numer Umowy podstawowej (Nazwa zadania)	Zakres powierzonych danych *(jakie dane zostały powierzone0*
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Z up. PREZYDENTA MIASTA

Andrzej Kacperek
WICEPREZYDENT MIASTA

Umowa powierzenia przetwarzania danych osobowych stanowiąca uzupełnienie Umowy .....zawartej w dniu .....r.

zawarta w dniu ..... w Piotrkowie Trybunalskim, między:

Miastem Piotrków Trybunalski, Pasaż Karola Rudowskiego 10, 97-300 Piotrków Trybunalski, reprezentowanym przez:

.....,

zwanym dalej Administratorem

a

.....,

reprezentowanym przez:

.....

Zwanej dalej Przetwarzającym

dalej łącznie jako strony.

Mając na uwadze, że

strony zawarły umowę (umowa podstawowa), w związku z wykonywaniem której Administrator powierzył Przetwarzającemu przetwarzanie danych osobowych a ich celem jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania danych osobowych w imieniu Administratora, zgodnie z zasadami przetwarzania danych osobowych, wynikającymi z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1) - dalej RODO,

strony postanowiły zawrzeć umowę o następującej treści:

§ 1

1. Na warunkach określonych niniejszą umową oraz umową podstawową Administrator powierza Przetwarzającemu przetwarzanie (w rozumieniu RODO) dalej opisanych danych osobowych (dalej w skrócie zwanych danymi).

2. Powierzone przez Administratora dane osobowe będą przetwarzane przez podmiot przetwarzający wyłącznie w celu wykonania przedmiotu umowy podstawowej.

3. Przetwarzanie będzie wykonywane w okresie obowiązywania umowy podstawowej.

§ 2

Przetwarzanie obejmować będzie dane osobowe .....
w tym: .....

§ 3

1. Przetwarzający może powierzyć konkretne operacje przetwarzania danych („podpowierzenie"), w drodze pisemnej umowy (umowa podpowierzenia) innym podmiotom przetwarzającym, pod warunkiem uprzedniej akceptacji przez Administratora lub braku jego sprzeciwu.

2. Powierzenie przetwarzania danych podprzetwarzającym wymaga uprzedniego zgłoszenia Administratorowi w celu umożliwienia wyrażenia sprzeciwu.

3. Administrator może z uzasadnionych przyczyn w ciągu 2 dni od otrzymania informacji o zamiarze podpowierzenia danych osobowych zgłosić sprzeciw wraz z uzasadnieniem przeciwko podpowierzeniu danych podprocesorowi.

5. W razie zgłoszenia sprzeciwu przetwarzający nie ma prawa powierzyć danych podprzetwarzającemu objętemu sprzeciwem, a jeżeli sprzeciw dotyczy aktualnego podprzetwarzającego, musi niezwłocznie zakończyć podpowierzenie temu podprzetwarzającemu. Wątpliwości co do zasadności sprzeciwu przetwarzający zgłosi Administratorowi w czasie umożliwiającym zapewnienie ciągłości przetwarzania.

6. Dokonując podpowierzenia, Przetwarzający ma obowiązek zobowiązać podprzetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej umowy powierzenia, z wyjątkiem tych, które nie mają zastosowania ze względu na naturę konkretnego podpowierzenia.

7. Przetwarzający nie ma prawa przekazać podprzetwarzającemu całości wykonania umowy.

§ 4

1. Przetwarzający przetwarza dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora.

2. Przetwarzający nie przekazuje danych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy - EOG) bez zgody Administratora.

3. Przetwarzający nie korzysta z podwykonawców, którzy przekazują dane poza EOG.

4.Przetwarzający uzyskuje od osób, które zostały upoważnione do przetwarzania danych w celu wykonania umowy, zobowiązania do zachowania tajemnicy, ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy.

5.Przetwarzający zapewnia ochronę danych i podejmuje środki ochrony danych, o których mowa w art. 32 RODO, zgodnie z dalszymi postanowieniami umowy.

6.Przetwarzający zobowiązuje się do odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III RODO (tzw. „prawa

jednostki"). Przetwarzający zapewnia obsługę praw jednostki w odniesieniu do powierzonych danych a szczegóły obsługi praw jednostki zostaną między stronami uzgodnione.

7.Przetwarzający współpracuje z Administratorem przy wykonywaniu przez Administratora obowiązków z obszaru ochrony danych osobowych, o których mowa w art. 32-36 RODO (ochrona danych, zgłaszanie naruszeń organowi nadzorczemu, zawiadamianie osób dotkniętych naruszeniem ochrony danych, ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym).

§ 5

Jeżeli Przetwarzający powezmie wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości, pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.

§ 6

Planując dokonanie zmian w sposobie przetwarzania danych, Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 RODO, i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i w takich terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany w opinii Administratora grożą uzgodnionemu poziomowi bezpieczeństwa danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania danych przez Przetwarzającego.

§ 7

1. Przetwarzający zobowiązuje się do ograniczenia dostępu do danych wyłącznie dla osób, których dostęp do danych jest potrzebny do realizacji umowy i posiadających odpowiednie upoważnienie.

2. Przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania danych odpowiednie szkolenie z zakresu ochrony danych osobowych.

§ 8

Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

§ 9

Dla realizacji niniejszej umowy Przetwarzający przeprowadził analizę ryzyka przetwarzania powierzonych danych, udostępnił ją Administratorowi i stosuje się do jej wyników co do organizacyjnych i technicznych środków ochrony danych, a nadto Przetwarzający przedstawił Administratorowi informacje potwierdzające, że Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków

technicznych i organizacyjnych. i dowody przedstawienia informacji dla potrzeb spełnienia wymogu rozłączalności.

§ 10

1. Przetwarzający powiadamia Administratora o każdym podejrzeniu naruszenia ochrony danych nie później niż w 24 godziny od pierwszego zgłoszenia, zapewnia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia lub jego braku.

2. Przetwarzający przesyła Administratorowi powiadomienie o stwierdzeniu naruszenia wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić mu spełnienie obowiązku powiadomienia organu nadzoru.

3. Administrator kontroluje sposób przetwarzania powierzonych danych przez Przetwarzającego, po uprzednim poinformowaniu go o planowanej kontroli. Administrator lub wyznaczone przez niego osoby są uprawnione do wstępu do pomieszczeń, w których przetwarzane są dane, oraz wglądu do dokumentacji związanej z przetwarzaniem danych.

4. Administrator uprawniony jest do żądania od Przetwarzającego niezwłocznego udzielania informacji dotyczących przebiegu przetwarzania danych oraz udostępnienia rejestrów przetwarzania (z zastrzeżeniem tajemnicy handlowej Przetwarzającego).

§ 11

1. Przetwarzający współpracuje z urzędem ochrony danych osobowych w zakresie wykonywanych przez niego zadań.

2. Przetwarzający:

(1) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania zgodności działania Administratora z przepisami RODO,

(2) umożliwia Administratorowi lub upoważnionemu audytorowi przeprowadzanie audytów lub inspekcji. Przetwarzający współpracuje w zakresie realizacji audytów lub inspekcji.

§12

1.Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego, lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom.

2.Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub niezastosowaniem właściwych środków bezpieczeństwa.

3. Jeżeli podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków przez podprzetwarzającego spoczywa na Przetwarzającym.

§ 13

1. Umowa obowiązuje przez czas trwania umowy podstawowej.

2. W przypadku zakończenia trwania umowy podstawowej, niezależnie od przyczyny, niniejsza umowa ulega wygaśnięciu z chwilą zakończenia obowiązywania umowy podstawowej.

3. Strony mogą rozwiązać umowę z zachowaniem miesięcznego okresu wypowiedzenia, liczonego na koniec miesiąca kalendarzowego, w którym doszło do wypowiedzenia.

§14

Z chwilą rozwiązania lub wygaśnięcia umowy Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych danych i jest zobowiązany do przekazania przetwarzanych w toku danych osobowych do Administratora, chyba że Administrator postanowi inaczej lub prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują dalej przechowywanie danych.

§ 15

1. W razie sprzeczności między postanowieniami niniejszej umowy powierzenia a umowy podstawowej pierwszeństwo mają postanowienia umowy powierzenia. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych między Administratorem a Przetwarzającym należy regulować przez zmiany niniejszej umowy lub w wykonaniu jej postanowień.

2. Wszelkie sprawy sporne wynikające z niniejszej umowy będzie rozstrzygał odpowiedni sąd w Piotrkowie Trybunalskim

3. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

.....

Administrator

.....

Przetwarzający

Z up. PREZYDENTA MIASTA

Andrzej Kacperek

WICEPREZYDENT MIASTA

Załącznik nr 7 do Polityki Bezpieczeństwa Informacji

WYKAZ UDOSTĘPNIEŃ DANYCH OSOBOWYCH INNYM PODMIOTOM

L.p.	**Imię i Nazwisko/Nazwa zbioru** *(możliwie najpełniejszy opis osoby, której dane zostały udostępnione lub całego zbioru)*	**Data udostępnienia**	**Nazwa podmiotu, któremu udostępniono dane**	**Cel udostępnienia** *(podstawa prawna/numer umowy)*	**Zakres udostępnionych danych** *(jakie dane zostały udostępnione)*	**Rodzaj zbioru/zasobu i jego lokalizacja** *(np. papierowy wydruk, dane w formie elektronicznej)*
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						

Z up. PREZYDENTA MIASTA

Andrzej Kasperek
WICEPREZYDENT MIASTA

Załącznik nr 8 do Polityki Bezpieczeństwa Informacji

Rejestr naruszeń ochrony Danych osobowych

Kod	Data i godzina zdarzenia	Rodzaj zdarzenia (uchybienie lub zagrożenie)	Opis zdarzenia	Skutki zdarzenia	Działania naprawcze

Z up. PREZYDENTA MIASTA
Andrzej Kacperek
WICEPREZYDENT MIASTA

Załącznik nr 9 do Polityki Bezpieczeństwa Informacji

PROTOKÓŁ NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Data i godzina wystąpienia zagrożenia .....

Kod zagrożenia .....

Opis zagrożenia

.....
.....
.....
.....
.....

Przyczyny powstania zagrożenia

.....
.....
.....
.....
.....

Zaistniałe skutki zagrożenia

.....
.....
.....
.....

Podjęte działania naprawczo-zapobiegawcze

.....
.....
.....
.....

Inspektor Ochrony Danych

.....

Administrator Danych Osobowych

.....

Z up. PREZYDENTA MIASTA
Andrzej Kacperek
WICEPREZYDENT MIASTA

Wymagania w zakresie bezpieczeństwa informacji dla kontrahentów oraz podmiotów współpracujących z Urzędem Miasta Piotrkowa Trybunalskiego

§ 1.

Wymagania w zakresie bezpieczeństwa informacji dla kontrahentów oraz podmiotów współpracujących z Urzędem Miasta stanowią dokument, którego celem jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych standardu przetwarzania informacji powierzanych kontrahentom oraz podmiotom współpracującym w związku z realizacją umów. Niniejszy dokument jest udostępniany każdemu kontrahentowi oraz podmiotowi współpracującemu przed zawarciem umowy.

§ 2.

Wymagania w zakresie bezpieczeństwa informacji dla kontrahentów oraz podmiotów współpracujących z Urzędem Miasta zostały opracowane w oparciu o:

1. Ustawa z dnia 10 maja 2018r., o ochronie danych osobowych (Dz. U. 2018 r. poz. 1000)
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024 z późn. zm.)
3. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie przez administratora bezpieczeństwa informacji (Dz.U. z 2015 roku, poz. 745 z późn. zm.)
4. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. 2015, poz. 719 z późn. zm.)
5. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2016 z roku, poz. 113 z późn. zm.)
6. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO)

§ 3.

Ilekroć w niniejszym dokumencie jest mowa o:

1. **Administratorze Danych Osobowych (ADO)** – należy przez to rozumieć organ, jednostkę organizacyjną, podmiot lub osobę decydujące o celach i środkach przetwarzania danych osobowych (kontrahenta);
2. **Inspektor Ochrony Danych (IOD)** - należy przez to rozumieć pracownika powołanego przez Administratora Danych Osobowych, zajmującego się zapewnianiem przestrzegania przepisów o ochronie danych osobowych oraz prowadzeniem rejestru przetwarzania i innej niezbędnej dokumentacji;
3. **Informatyku (Administratorze Systemów Informatycznych – ASI)** – należy przez to rozumieć wyznaczoną przez ADO osobę fizyczną odpowiedzialną za bezpieczeństwo

organizacyjne, fizyczne oraz techniczne danych osobowych przetwarzanych w systemie informatycznym;

4. **Kontrahencie/podmiocie współpracującym** – należy przez to rozumieć stronę umowy;
5. **Danych osobowych** – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
6. **UODO** – należy przez to rozumieć Urząd Ochrony Danych Osobowych.
7. **IZSI/Instrukcji** – należy przez to rozumieć obowiązujący u kontrahenta dokument o nazwie Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
8. **Nośnikach danych** – należy przez to rozumieć przedmioty fizyczne (elektroniczne, papierowe), na których możliwe jest zapisanie informacji w celu ich przechowywania, przetwarzania i transmisji;
9. **Odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią z wyłączeniem organów publicznych które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego. Przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
10. **PBI / Polityce** – należy przez to rozumieć obowiązujący u kontrahenta dokument regulujący zasady bezpiecznego przetwarzania danych osobowych, zgodny z wymogami przepisów prawa, o których mowa w § 2 ust. 1-7;
11. **Pracowniku** – należy przez to rozumieć osobę fizyczną świadczącą pracę lub wykonującą czynności w oparciu o zawarte umowy cywilnoprawne w/na rzecz kontrahenta;
12. **Przetwarzaniu danych** – należy przez to rozumieć wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemie informatycznym;
13. **Systemie informatycznym (Systemie IT)** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych u kontrahenta w celu przetwarzania danych osobowych;
14. **Użytkowniku** – należy przez to rozumieć osobę, która uzyskała upoważnienie od kontrahenta do przetwarzania danych osobowych w systemie informatycznym oraz podpisała oświadczenie o zachowaniu poufności zobowiązującym ją do zachowania w tajemnicy przetwarzanych danych;

§ 4.

Wymagania w zakresie bezpieczeństwa informacji dla kontrahentów oraz podmiotów współpracujących z Urzędem Miasta określają kryteria zapewnienia przez kontrahentów oraz podmioty współpracujące bezpieczeństwa informacjom zawierającym dane osobowe, niezbędne środki organizacyjne i techniczne zapewniające ochronę tych danych, reguły postępowania w sytuacji naruszenia ich bezpieczeństwa oraz konsekwencje naruszenia

przepisów o ochronie danych osobowych przez kontrahentów, ich pracowników oraz pozostałe osoby upoważnione przez kontrahentów do przetwarzania tych danych.

§ 5.

Utrzymanie bezpieczeństwa informacji, w tym w szczególności bezpieczeństwa danych osobowych przetwarzanych przez kontrahenta rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na poziomie wymaganym przepisami prawa.

§ 6.

Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych. Zarządzanie ryzykiem rozumiane jest jako proces identyfikowania, monitorowania i minimalizowania lub eliminowania ryzyka, które może dotyczyć systemów informatycznych i tradycyjnych służących do przetwarzania danych osobowych.

§ 7.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, pełni funkcję kontrolną w zakresie poprawnego przetwarzania danych osobowych oraz jest odpowiedzialny za zapewnienie środków organizacyjnych i technicznych służących utrzymaniu poziomu bezpieczeństwa tych danych, zgodnie w wymaganiami określonymi w przepisach prawa.

§ 8.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do prowadzenia aktualnej i zgodnej z przepisami prawa dokumentacji w zakresie przetwarzania danych osobowych.

§ 9.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do ujawnienia obowiązujących u niego zasad w zakresie:

1) wypełniania obowiązku informacyjnego, wynikającego z przepisów prawa,
2) zastosowanych środków technicznych i organizacyjnych służących zachowaniu szczególnej staranności przy przetwarzaniu danych osobowych,
3) możliwości aktualizowania przetwarzanych danych osobowych, czasowego lub stałego wstrzymania przetwarzania danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane,
4) nadawania i anulowania upoważnień do przetwarzania danych osobowych oraz zgodności stosowanych upoważnień z wymaganiami określonymi w przepisach prawa,
5) ewidencjonowania osób upoważnionych do przetwarzania danych osobowych (wykaz osób upoważnionych do przetwarzania danych osobowych),
6) zobowiązywania osób upoważnionych do przetwarzania danych osobowych do zachowania ich w tajemnicy z określeniem okresu obowiązywania tego zobowiązania (oświadczenie o zachowaniu poufności),
7) sprawowania kontroli nad udostępnianiem i powierzaniem danych osobowych oraz prowadzenia wymaganej przepisami dokumentacji w tym zakresie.

§ 10.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do przekazania informacji o wypełnieniu formalności związanych z wyznaczeniem Inspektora Ochrony Danych.

§ 11.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do określenia w dokumentacji bezpieczeństwa informacji kompetencji - Inspektora Ochrony Danych.

§ 12.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do opracowania zasad prowadzenia przez Inspektora Ochrony Danych jawnego rejestru danych osobowych.

§ 13.

Inspektor Ochrony Danych pełniący obowiązki u/na rzecz kontrahenta / podmiotu współpracującego zobowiązany jest do cyklicznego (nie rzadziej niż jeden raz w roku) przeprowadzania analizy ryzyk związanych z zagrożeniami związanymi z przetwarzaniem danych osobowych oraz prowadzenia dokumentacji w tym zakresie.

§ 14.

Inspektor Ochrony Danych pełniący obowiązki u/na rzecz kontrahenta / podmiotu współpracującego jest ponadto odpowiedzialny za prowadzenie i aktualizację dokumentacji w postaci:

1) wykazu pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania,
2) wykazu udostępnień danych osobowych innym podmiotom,
3) wykazu podmiotów, którym powierzono dane osobowe do przetwarzania,
4) wykazu udostępnień danych osobowych osobom, których dane dotyczą.

§ 15.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do wyznaczenia osoby (informatyka, administratora systemu), zobowiązanej do sprawowania nadzoru nad bezpieczeństwem informacji przetwarzanych w systemie informatycznym stosowanym u kontrahenta / w podmiocie współpracującym.

§ 16.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do opracowania dokumentacji w postaci Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, określającej procedury

nadawania uprawnień do przetwarzania danych osobowych przez użytkowników tego systemu, metody i środki uwierzytelniania, zasady konfiguracji oraz użytkowania sprzętu stacjonarnego oraz urządzeń mobilnych i elektronicznych nośników danych przez użytkowników systemu oraz zasady zabezpieczania danych w systemie informatycznym.

§ 17.

Kontrahent / podmiot współpracujący, jako Administrator Danych Osobowych, zobowiązany jest do opracowania procedur tworzenia i przechowywania kopii zapasowych, wykonywania przeglądów, konserwacji i napraw sprzętu wchodzącego w skład systemu informatycznego oraz zasad postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa tego systemu.

§ 18.

W sprawach nieuregulowanych niniejszym dokumentem mają zastosowanie przepisy prawa wymienione w § 2 ust. 1 – 7.

Z up. PREZYDENTA MIASTA
Andrzej Kacperek
WICEPREZYDENT MIASTA