Załącznik Nr 1
do Zarządzenia Burmistrza Jarocina
Nr 415/VII/2018.K
z dnia 21 czerwca 2018r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w URZĘDZIE MIEJSKIM W JAROCINIE

Część I – Wstęp

§ 1

Zgodnie z art. 32 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) zwanej dalej „RODO" ustanawia się „Politykę Bezpieczeństwa".

§ 2

Ilekroć w niniejszym dokumencie jest mowa o jednostce organizacyjnej, należy przez to rozumieć **Urząd Miejski w Jarocinie reprezentowany przez Burmistrza Jarocina** zwanym dalej Administratorem Danych Osobowych (ADO)

§ 3

Podstawowe pojęcia dotyczące ochrony danych osobowych zostały określone w ogólnym rozporządzeniu o ochronie danych osobowych oraz Polityce Bezpieczeństwa Informacji.

§ 4

Każda osoba, mająca dostęp do danych osobowych przetwarzanych w jednostce organizacyjnej jest zobowiązana do zapoznania się z niniejszym dokumentem oraz stosowania do jego przepisów.

Część II – Cel i zasady przetwarzania i ochrony danych osobowych

§ 1

Celem niniejszej Polityki Bezpieczeństwa jest wdrożenie organizacyjnych i technicznych środków bezpieczeństwa dla zapewnianie przetwarzania danych się zgodnie z przepisami ogólnego rozporządzenia o ochronie danych oraz minimalizacja ryzyka praw i wolności osób fizycznych.

§ 2

Zgodnie z Polityką Bezpieczeństwa Informacji przyjmuje się następującą definicję bezpieczeństwa: przez bezpieczeństwo aktywów rozumiemy zapewnienie ochrony następujących ich cech:

1. **Poufności** – właściwości zapewniającej, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom albo procesom.
2. **Integralności danych** – właściwości zapewniającej, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
3. **Integralności systemu** – właściwości polegającej na tym, że system realizuje swoją zamierzoną funkcję w sposób nienaruszony, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.
4. **Dostępności** – właściwości bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowanych użytkowników.
5. **Autentyczności** – właściwości zapewniającej, że tożsamość użytkownika lub zasobu jest taka, jak deklarowana.
6. **Niezawodności** – właściwości oznaczającej spójne, zamierzone zachowanie systemu w różnych warunkach
7. **Niezaprzeczalności** – właściwości oznaczającej brak możliwości wyparcia się swojego uczestnictwa w całości lub części procesu wymiany danych
8. **Rozliczalności** - właściwości zapewniającej, że określone działania dowolnego podmiotu mogą być jednocześnie przypisane temu podmiotowi

§ 3

Administrator danych przetwarza dane osobowe z poszanowaniem następujących zasad:

1. W oparciu o podstawę prawną i zgodnie z prawem (zasada legalizmu)
2. Rzetelnie i uczciwie (zasada rzetelności)

3. Sposób przejrzysty dla osoby, której dane dotyczą (zasada transparentności)
4. W konkretnych celach (zasada minimalności)
5. Nie więcej niż potrzeba (zasada adekwatności)
6. Z dbałością o prawidłowość danych (zasada prawidłowości)
7. Nie dłużej niż potrzeba (zasada czasowości)
8. Zapewniając odpowiednie bezpieczeństwo danych (zasada bezpieczeństwa)

Część III – System ochrony (inwentaryzacja danych)

§ 1

Administrator dokonuje identyfikacji zasobów danych osobowych, klas, zależności między nimi identyfikacji sposobów ich wykorzystania uwzględniając:

1. Możliwość przetwarzania szczególnych kategorii danych osobowych (dane wrażliwe);
2. Podstawy prawne przetwarzania;
3. Przypadków przetwarzania danych dzieci;
4. Profilowania i przetwarzania automatycznego;
5. Współadministrowania danymi;
6. Powierzenia przetwarzania danych;

§ 2

Administrator dokumentuje procesy przetwarzania i prowadzi wymagany przez ogólne rozporządzenie o ochronie danych rejestr czynności przetwarzania danych osobowych zgodnie z załącznikiem nr 1 do niniejszej polityki.

§ 3

W przypadku powierzenia administratorowi przetwarzania danych osobowych administrator dokumentuje procesy przetwarzania i prowadzi wymagany przez ogólne rozporządzenie o ochronie danych rejestr kategorii czynności przetwarzania danych osobowych zgodnie z załącznikiem nr 2 do niniejszej polityki.

§ 4

W celu minimalizacji ryzyka oraz zapewniania adekwatnych organizacyjnych i technicznych środków ochrony administrator wykonuje analizę ryzyka zgodnie z Instrukcją Analizy Ryzyka opisaną w załączniku nr 1 do Polityki Bezpieczeństwa Informacji.

Analiza ryzyka wymagana jest każdorazowo w przypadku przetwarzania nowych zbiorów danych osobowych, zmian w systemie informatycznym, wdrożenia nowych rozwiązań informatycznych, istotnych zmian organizacyjnych. Zaleca się okresowe przeglądy ryzyka.

§ 5

W przypadku gdy dany rodzaj przetwarzania może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych administrator wykonuje ocenę skutków dla ochrony danych zgodnie z zasadami określonymi w art. 35 ogólnego rozporządzenia o ochronie danych osobowych. Dla oceny zalecane jest wykorzystanie z metody analizy ryzyka zgodnie z Instrukcją Analizy Ryzyka opisaną w załączniku nr 1 do Polityki Bezpieczeństwa Informacji. W przypadku stwierdzenia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych na zasadach określonych w art. 36 ogólnego rozporządzenia o ochronie danych osobowych administrator zobowiązany jest przeprowadzić konsultacje z Prezesem Urzędu Ochrony Danych Osobowych.

§ 6

Zasady bezpieczeństwa określone w dokumentacji bezpieczeństwa stosuje się na każdym etapie przetwarzania w tym na etapie określania sposobów przetwarzania danych w tym na etapach planowania i projektowania przetwarzania (zasada ochrony danych w fazie projektowania)

Część IV - Organizacyjne i techniczne środki ochrony

§ 1

Za zapewnienie bezpieczeństwa odpowiada administrator danych. Administrator systemu informatycznego odpowiada za bezpieczeństwo danych przetwarzanych w systemach informatycznych. Każdy pracownik odpowiada za bezpieczeństwo stosowanie do posiadanych upoważnień i obowiązków.

§ 2

Przetwarzanie danych osobowych odbywa się na polecenie administratora danych na podstawie pisemnego upoważnienia wydanego zgodnie z załącznikiem nr 3 do niniejszego dokumentu. Pracownicy zobowiązani są podpisać oświadczenie o zachowaniu poufności tych danych zgodnie z załącznikiem nr 4 do niniejszego dokumentu.

§ 3

Osoby upoważnione do przetwarzania danych mają obowiązek:

a) przetwarzać je zgodnie z obowiązującymi przepisami, w szczególności z ustawą i rozporządzeniem

b) nie udostępniać ich oraz uniemożliwiać dostęp do nich osobom nieupoważnionym

c) zabezpieczać je przed zniszczeniem

§ 4

Każda osoba posiadająca upoważnienie do przetwarzania danych osobowych posiada swój identyfikator oraz hasło, pozwalające na zalogowanie się do systemu informatycznego, w którym przetwarzane są dane osobowe. Techniczne wymagania, jakie musi spełniać hasło, określone zostały w części w załączniku nr 4 do Polityki Bezpieczeństwa Informacji.

§ 5

W przypadku konieczności dostępu do obszaru przetwarzania osób, nieposiadających upoważnienia, o jakim mowa w § 4 (załącznik nr 3 do niniejszego dokumentu), które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują oni oświadczenie o zachowaniu poufności (załącznik nr 4 do niniejszego dokumentu).

§ 6

Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie w ramach umowy powierzenia przetwarzania danych osobowych, zgodnie z art. 28 oraz 29 RODO. Wzór umowy powierzenia przetwarzania danych osobowych zawarty jest w załączniku nr 10 do niniejszego dokumentu

§ 7

Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia, przez co rozumie się w szczególności pisemny wniosek podmiotu uprawnionego.

§ 9

Pracownicy zobowiązani są do stosowania się do zasady czystego biurka, a w przypadku przetwarzania danych w systemach informatycznych do zasady czystego ekranu. Dokumenty zawierające dane osobowe przechowywane w formie papierowej, przechowane są w szafach zamykanych na klucz. W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenie dokonuje się poprzez pocięcie w niszczarce.

§ 10

Zasady przetwarzania danych osobowych w systemie informatycznym określone są zawarte w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w **Urzędzie Miejskim w Jarocinie**".

§ 11

Nadzór nad przetwarzaniem danych osobowych w jednostce organizacyjnej sprawuje Inspektor ochrony danych (zwany dalej „IOD") wyznaczony przez Administratora Danych Osobowych. Upoważnienie wyznaczające IOD stanowi załącznik nr 5 do niniejszego dokumentu. IOD jest również zobowiązany do podpisania oświadczenia, stanowiącego załącznik nr 4 do niniejszego dokumentu.

§ 12

W celu podnoszenia świadomości pracowników w zakresie bezpieczeństwa przetwarzania danych osobowych inspektor ochrony danych informuje pracowników o spoczywających na nich obowiązkach w zakresie ochrony danych w szczególności o obowiązujących przepisach prawa, ich zmianach, występujących zagrożeniach, metodach zabezpieczeń. Informowanie może być realizowane w formie szkoleń, rozmów, opracowanych biuletynów informacyjnych, procedur, instrukcji, analiz.

§ 13

Administrator danych prowadzi również następujące wykazy:

a) ewidencję osób, którym nadano upoważnienia do przetwarzania danych osobowych - załącznik nr 6 do niniejszego dokumentu

b) wykaz podmiotów którym powierzono przetwarzanie danych osobowych – załącznik nr 7 do niniejszego dokumentu

c) rejestr naruszeń ochrony (incydentów) – załącznik nr 8 do niniejszego dokumentu

Część V - Obowiązki informacyjne

§ 1

Administrator realizuje obowiązki informacyjne wynikające z art. 13 i 14 ogólnego rozporządzenie o ochronie danych osobowych publikację klauzul informacyjnych zawierających między innymi następujące informacje:

a) tożsamość i dane kontaktowe tj. nazwę, dane adresowe, nr telefonu oraz adres e-mail

b) informację o powołaniu inspektora ochrony danych osobowych.

c) celu zbierania danych oraz podstawę prawną przetwarzania. Jeżeli ma zastosowanie, oprócz podstawy prawnej wynikającej z ogólnego rozporządzenie o ochronie danych należy wskazać podstawę szczegółową.

d) Informację o odbiorcach danych jeżeli istnieją

e) Prawach przysługujących osobie fizycznej

§ 2

Obowiązki informacyjne realizowane są na stronach biuletynu informacji publicznej oraz poprzez wywieszanie klauzul informacyjnych w dostępnych publicznie gablotach a także na stanowisku przetwarzania danych . Wzór podstawowej klauzuli informacyjnej zawarty jest w załączniku nr 9 do niniejszej polityki

§ 3

W przypadku otrzymania wniosku o udostępnienie danych osobowych od osoby, której one dotyczą, wyznaczona przez Administratora Danych Osobowych osoba przygotowuje odpowiedź w ciągu 30 dni.

Część VI - Naruszenia ochrony

§ 1

Każdy pracownik jest zobowiązany do reagowania na każdy stwierdzony fakt naruszenia bądź możliwości naruszenia ochrony danych, w szczególności:

1) nieautoryzowany (nieuprawniony) dostęp do danych

2) nieautoryzowane (nieuprawnione) modyfikacje lub zniszczenie danych
3) udostępnienie nieautoryzowanym (nieuprawnionym) podmiotom
4) nielegalne ujawnienie danych
5) pozyskiwanie danych z nielegalnych źródeł
6) stworzenie zagrożenia udostępnienia danych osobowych osobom nieuprawnionym.
7) otrzymanie podejrzanej korespondencji
8) zauważone nieprawidłowości w działaniu systemów informatycznych

§ 2

Osoba, która wykryła fakt naruszenia bądź możliwości naruszenia ochrony danych zgłasza to niezwłocznie osobie upoważnionej, administratorowi systemu informatycznego zgodnie z Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miejskim w Jarocinie. Zgłoszenia te są obsługiwane niezwłocznie.

§ 3

Administrator przy współudziale IOD dokonuje oceny naruszenia. Jeżeli nie występuje małe prawdopodobieństwo by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych administrator bez zbędnej zwłoki zgłasza naruszenie Prezesowi Urzędu Ochrony Danych Osobowych.

§ 4

Administrator prowadzi rejestr naruszeń ochrony danych zgodnie ze wzorem stanowiącym zawartym w załączniku nr 10 do niniejszego dokumentu.

Część VII - Okresowe przeglądy

§ 1

Administrator dokonuje okresowych przeglądów niniejszej polityki bezpieczeństwa. Polityka powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych administrator wykonuje przegląd polityki bezpieczeństwa stosownie do potrzeb.

§ 2

Przegląd polityki bezpieczeństwa ochrony danych osobowych musi uwzględnić adekwatność dokumentacji do:

1. zmian w systemie informatycznym,
2. zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,
3. zmian w obowiązującym prawie.

§ 3

Przegląd polityki bezpieczeństwa administrator wykonuje we współpracy z inspektorem ochrony danych. Stosownie do potrzeb administrator zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

Część VIII – Postanowienia końcowe

§ 1

Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z art. 83 RODO.

§ 2

W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy RODO.

§ 3

Niniejszy dokument wchodzi w życie z dniem 21.06.2018r.

……..……

podpis Administratora Danych Osobowych