Załącznik nr 1
do Zarządzenia Burmistrza Miasta Kościerzyna
nr 0050.196.2018 z dnia 07.12.2018 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI
Urzędu Miasta Kościerzyna

Właściciel dokumentu

. . . . . .
Sekretarz Miasta Kościerzyna

Zatwierdzający dokument

. . . . . .
Burmistrz Miasta Kościerzyna

Kościerzyna - 2018

WSTĘP

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – 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).

Ochrona przetwarzanych danych osobowych rozumiana jest natomiast jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Przy czym przez:

- poufność danych należy rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
- integralność danych należy rozumieć właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- rozliczalność danych należy rozumieć właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
- dostępność informacji należy rozumieć zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne.

§ 1

Administratorem Danych Osobowych (ADO) w Urzędzie Miasta Kościerzyna jest Burmistrz Miasta Kościerzyna. ADO w ramach swoich kompetencji pełni również rolę IOD, może wyznaczyć Inspektora ochrony danych (IOD), który w jego imieniu będzie odpowiedzialny za całościowy proces nadzoru nad zabezpieczeniem procesu przetwarzania danych osobowych, w tym zapewnienia integralności, rozliczalności oraz poufności danych. Rolę IOD może pełnić również podmiot zewnętrzny po uprzednim zawarciu stosownej umowy. Wyznaczony przez ADO IOD podlega mu bezpośrednio.

§ 2

Ilekroć w niniejszym dokumencie jest mowa o:

1) Urzędzie – należy przez to rozumieć Urząd Miasta Kościerzyna;
2) Ustawie – należy przez to rozumieć Ustawę o ochronie danych osobowych z dnia 10 maja 2018 roku (Dz. U. 2018 poz. 1000);
3) Rozporządzeniu (RODO) – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
4) Dane – oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu;
5) Dane szczególnej kategorii – oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
6) Podmiot przetwarzający – oznacza instytucję lub osobę, której Urząd powierzył przetwarzanie danych osobowych;
7) ADO – Administrator danych osobowych;
8) IOD – Inspektor ochrony danych;
9) ASI – Administrator systemów informatycznych;

10) System informatyczny – oznacza zespół współpracujących ze sobą urządzeń, programów, narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
11) System tradycyjny – oznacza zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia oraz środków trwałych w celu przetwarzania danych osobowych na papierze;
12) RCPD lub Rejestr – oznacza Rejestr Czynności Przetwarzania Danych Osobowych;
13) UODO – Urząd Ochrony Danych Osobowych.

§ 3

Celem niniejszego dokumentu jest zapewnienie zgodności procesu przetwarzania danych osobowych w Urzędzie z obowiązującymi przepisami prawa, w szczególności z RODO oraz Ustawą, a co za tym idzie zapewnienie przetwarzania tych danych w sposób gwarantujący ich bezpieczeństwo.

Regulacje wewnętrzne zawarte w niniejszym dokumencie określają środki i sposoby ochrony danych osobowych przyjętych przez ADO. Zmiany organizacyjne, zmiany sposobu działania ADO w zakresie mającym wpływ na proces przetwarzania danych osobowych oraz zmiany przepisów prawa będą powodowały konieczność aktualizacji niniejszego dokumentu.

Niniejszą Politykę stosuje się w odniesieniu do wszelkich danych osobowych, wobec których Urzędowi przysługuje status ADO, przetwarzanych zarówno w systemach informatycznych, jak i w systemach tradycyjnych (papierowych) tj. księgach, skorowidzach, wykazach i innych zbiorach ewidencyjnych, w szczególności danych osobowych przetwarzanych w celach rekrutacyjnych, zatrudnienia i nawiązania współpracy, finansowych i rachunkowych, świadczenia usług, realizacji działań marketingowych oraz windykacyjnych.

Zakres stosowania Polityki obejmuje ponadto:

a) wszystkie lokalizacje Urzędu – budynki i pomieszczenia, w których są lub będą przetwarzane informacje podlegające ochronie,

b) wszystkich pracowników Urzędu w rozumieniu przepisów Kodeksu pracy, współpracowników, praktykantów, stażystów oraz innych osób mających dostęp do informacji podlegających ochronie,

c) Radnych Gminy Miejskiej Kościerzyna,

d) Podmioty przetwarzające.

Niniejszy dokument podlega przeglądom i aktualizacji, w szczególności w przypadku wystąpienia zmian w przepisach prawa oraz w przypadku wprowadzania zmian w działaniach ADO związanych z przetwarzaniem danych osobowych.

§ 4

1. Na ADO spoczywa odpowiedzialność za realizację szeregu zadań wynikających z RODO. Są to w szczególności takie zadania jak:

   a) utworzenie odpowiednich klauzul informacyjnych wynikających z obowiązków ADO zawartych w art. 13-14 RODO (art. 12),

b) ułatwianie podmiotom danych wykonywania ich praw wynikających z art. 15 – 22 RODO (art. 15 – 22),
c) wdrożenie i uaktualnianie niniejszej dokumentacji wraz z procedurami ochrony danych (art. 24),
d) uwzględnianie ochrony danych w fazie projektowania (art. 25),
e) wyznaczanie podmiotów przetwarzających dane osobowe na podstawie umowy lub innego aktu prawnego (art. 28),
f) weryfikacja i uaktualnienie upoważnień do przetwarzania danych osobowych (art. 28),
g) prowadzenie rejestru czynności przetwarzania danych (art. 30),
h) współpraca z organem nadzorczym – UODO (art. 31),
i) analiza ryzyk naruszenia praw podmiotów danych (art. 32),
j) wdrożenie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa przetwarzania danych odpowiadającego analizowanym ryzykom (art. 32),
k) zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu (art. 33),
l) prowadzenie rejestru naruszeń ochrony danych osobowych (art. 33),
m) zawiadamianie podmiotów danych o naruszeniach ochrony ich danych osobowych (art. 34),
n) opracowanie dokumentacji określanej jako „ocena skutków dla ochrony danych" w przypadkach wymienionych w art. 35 RODO (art. 35),
o) prowadzenie tzw. „uprzednich konsultacji" z organem nadzorczym w przypadku wymienionym w art. 36 RODO (art. 36),
p) wyznaczenie Inspektora ochrony danych – IOD (art. 37).

Wskazane powyżej zadania ADO może w całości lub w części powierzyć IOD.

2. Do zadań IOD w szczególności należy:
   a) weryfikacja procesów przetwarzania danych z uwzględnieniem zasad wskazanych w RODO,
   b) identyfikacja i aktualizacji zbiorów danych osobowych,
   c) przeprowadzenie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych oraz monitorowanie jej wykonania – w rozumieniu art. 35 RODO,
   d) opracowanie klauzul zgód na przetwarzanie danych osobowych oraz klauzul obowiązków informacyjnych, a w razie potrzeby przygotowanie niezbędnych zmian lub opracowanie właściwych dokumentów i klauzul,
   e) analiza techniczno-organizacyjnych środków ochrony bezpieczeństwa fizycznego oraz informatycznego związanych z przetwarzaniem danych osobowych,
   f) prowadzenie rejestru czynności lub rejestru kategorii czynności przetwarzania danych osobowych - w rozumieniu art. 30 RODO,
   g) zarządzanie uprawnieniami do przetwarzania danych osobowych,
   h) zarządzanie ewidencją osób upoważnionych do przetwarzania danych osobowych,
   i) informowanie ADO oraz pracowników Urzędu, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub przepisów prawa krajowego o ochronie danych i doradzanie im w tej sprawie,
   j) monitorowanie przestrzegania RODO, innych przepisów Unii, przepisów prawa krajowego o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość,
   k) prowadzenie korespondencji z organem nadzorczym,
   l) udzielanie na żądanie ADO zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO,
   m) opiniowanie dokumentów, informacji wytworzonych lub przetwarzanych przez ADO pod kątem zgodności z RODO, np. umów, odpowiedzi udzielanych osobom trzecim w trybie

przepisów o dostępie do informacji publicznej,

n) prowadzenie szkoleń z zakresu ochrony danych osobowych dla pracowników ADO uczestniczących w operacjach przetwarzania oraz powiązane z tym audyty,
o) wspieranie pracy audytorów zewnętrznych w zakresie ochrony danych osobowych;
p) udział w kontrolach organu nadzorczego oraz współpraca z organem nadzorczym;
q) udział w kontrolach prowadzonych u ADO przez innych administratorów danych;
r) prowadzenie audytów podmiotów, którym Zleceniodawca powierzył przetwarzanie danych osobowych;
s) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszystkich innych sprawach,
t) pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO – zgodnie z art. 38 ust. 4 RODO.

3. Do zadań ASI w szczególności należy:

a) współpraca przy przygotowaniu i wdrażaniu dokumentacji ochrony danych osobowych,
b) współpraca przy przeprowadzaniu okresowych audytów związanych z przetwarzaniem danych osobowych,
c) zapewnienie ciągłości działania systemów,
d) zapewnienie awaryjnego źródła zasilania oraz zabezpieczenia przed zakłóceniami w sieci zasilającej,
e) nadzór nad naprawą oraz likwidacją urządzeń komputerowych oraz nośników danych,
f) nadzór nad przeglądami i konserwacjami systemów informatycznych służących do przetwarzania danych osobowych,
g) zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem oprogramowania złośliwego,
h) dostosowanie systemów informatycznych służących do przetwarzania danych osobowych do wymogów RODO,
i) zabezpieczenie pomieszczenia serwerowni przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych,
j) ochrona przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,
k) zabezpieczenie nośników informacji (np. dyski twarde, pamięci USB),
l) weryfikacja poprawności działania programów antywirusowych.

§ 5

1. Każda osoba mająca dostęp do danych osobowych przetwarzanych w Urzędzie zobowiązana jest do podpisania oświadczenia o zachowaniu poufności tych danych. Wzór oświadczenia stanowi załącznik nr 2 do niniejszego dokumentu.
2. Osoby zatrudnione w Urzędzie, które przetwarzają dane osobowe i podpisały oświadczenie o zachowaniu poufności tych danych, muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez Administratora Danych Osobowych (ADO). Wzór upoważnienia stanowi załącznik nr 1 do niniejszego dokumentu.
3. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych w Urzędzie zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO oraz niniejszej Polityki ochrony danych.

4. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich przetwarzania i zabezpieczenia. Obowiązek ten istnieje także po ustaniu stosunku zatrudnienia oraz świadczenia usług.

§ 6

1. Filary ochrony danych osobowych w Urzędzie:

   a) **Legalność** – Urząd dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
   b) **Bezpieczeństwo** – Urząd zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie.
   c) **Prawa jednostki** – Urząd umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
   d) **Rozliczalność** – Urząd dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność z obowiązującymi przepisami.

2. Zasady ochrony danych.

Urząd przetwarza dane osobowe z poszanowaniem następujących zasad:

   a) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
   b) rzetelnie i uczciwie (rzetelność);
   c) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
   d) w konkretnych celach i nie „na zapas" (minimalizacja);
   e) nie więcej niż potrzeba (adekwatność);
   f) z dbałością o zgodność danych (prawidłowość);
   g) nie dłużej niż potrzeba (czasowość);
   h) zapewniając odpowiednie zabezpieczenie danych (bezpieczeństwo).

Osoby upoważnione do przetwarzania danych mają obowiązek zabezpieczania danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 7

1. Obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania) stanowią wszystkie pomieszczenia biurowe zajmowane przez komórki organizacyjne Urzędu z wyłączeniem pomieszczeń gospodarczych i korytarzy w budynkach:
   a) przy ul. 3 Maja 9a w Kościerzynie,
   b) przy ul. Młyńskiej 15 w Kościerzynie.
2. W przypadku konieczności uzyskania dostępu do obszaru przetwarzania przez osoby nieupoważnione do przetwarzania danych osobowych, które muszą wykonać prace o charakterze serwisowym lub inne działania doraźne, osoby te są zobowiązane są do złożenia oświadczenie o zachowaniu poufności, o którym mowa wyżej w § 5 ust 1.
3. Osoby nieupoważnione mogą przebywać w obszarach określonych, jako obszar przetwarzania wyłącznie w obecności osoby upoważnionej do przetwarzania danych osobowych będącej pracownikiem Urzędu.
4. Przebywanie w pomieszczeniach serwerowni Urzędu innych osób niż ASI dopuszczalne jest tylko w obecności ASI lub za jego pisemną zgodną. Zasada ta dotyczy również osób wykonujących czynności serwisowe niezbędne dla funkcjonowania infrastruktury technicznej lub upoważnionych do prowadzenia kontroli.

5. Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych może nastąpić wyłącznie na podstawie zawartej na piśmie umowy powierzenia przetwarzania danych osobowych. Do zawierania takich umów upoważniony jest jedynie ADO w porozumieniu z IOD.

§ 8

1. IOD (realizując zadania na rzecz Urzędu) opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Urzędzie. Wzór RCPD stanowi załącznik nr 8 do niniejszego dokumentu.
2. IOD (realizując zadania na rzecz Urzędu) zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
   - utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,
   - inwentaryzuje i uszczegóławia uzasadnienie przypadków przetwarzania danych na podstawie prawnie uzasadnionego interesu.
3. IOD (realizując zadania na rzecz Urzędu) spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a) obowiązki informacyjne – przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;
   b) możliwość wykonania żądań – weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających;
   c) obsługa żądań – zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO oraz dokumentowane;
   d) zawiadamianie o naruszeniach – stosuje zasady pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

Zarządzanie zgodami umożliwia rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (e-mail, telefon, SMS itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

4. Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie na pisemny wniosek podmiotu i po pozytywnym zweryfikowaniu ustawowych przesłanek dopuszczalności takiego udostępnienia.

§ 9

1. Każda osoba posiadająca dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe musi posiadać w tym systemie swój unikalny identyfikator oraz indywidualne hasło.
2. Niedozwolone jest przetwarzanie danych osobowych na komputerach przenośnych nieposiadających adekwatnych poziomów zabezpieczeń poza obszarem przetwarzania, o którym mowa w § 7 ust.1.
3. Wycofane z użycia nośniki danych należy przekazać do ASI.
4. Urząd zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
   - przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii. Wzór rejestru ryzyka stanowi załącznik nr 7 do niniejszego dokumentu;
   - przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
   - dostosowuje środki ochrony danych do ustalonego poziomu ryzyka;
   - posiada system zarządzania bezpieczeństwem informacji;
   - stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych Osobowych – zarządza incydentami.

5. Szczegółowe zasady przetwarzania danych osobowych w systemie informatycznym określone są w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Kościerzyna”.

§ 10

1. Dokumenty zawierające dane osobowe przechowywane w formie papierowej upoważnione osoby przechowują w obszarze przetwarzania danych w szafach w pomieszczeniach zamykanych na klucz.
2. W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenie dokonuje się wyłącznie z użyciem niszczarek.

§ 11

1. Rejestr Czynności Przetwarzania Danych stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
2. IOD (realizując zadania na rzecz Urzędu) prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Rejestr jest jednym z podstawowych narzędzi umożliwiających rozliczanie większości obowiązków ochrony danych.
3. W Rejestrze dla każdej czynności przetwarzania danych, którą uznano za odrębną dla potrzeb Rejestru, odnotowuje się:

   a) nazwę czynności,
   b) cel przetwarzania,
   c) opis kategorii osób,
   d) opis kategorii danych,
   e) podstawę prawną przetwarzania,
   f) sposób zbierania danych,
   g) opis kategorii odbiorców danych (w tym przetwarzających),
   h) informację o przekazaniu poza EU/EOG,
   i) ogólny opis technicznych i organizacyjnych środków ochrony danych.

4. W rejestrze udokumentowane są podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
5. Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne / władza publiczna, prawnie uzasadniony interes), dookreśla się podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne.

§ 12

1. Realizując prawa osób, których dane dotyczą, Urząd w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste), może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
2. Nieprzetwarzanie – Urząd informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

3. Odmowa – Urząd informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
4. Dostęp do danych – na żądanie osoby, dotyczące dostępu do jej danych, Urząd informuje osobę, czy przetwarza jej dane, oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Urząd nie uzna za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
5. Kopia danych – na żądanie osoby Urząd wydaje kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.
6. Sprostowanie danych – Urząd dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Urząd ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Urząd informuje osobę o odbiorcach danych, na żądanie tej osoby.
7. Uzupełnienie danych – Urząd uzupełnia i aktualizuje dane na żądanie osoby. Urząd ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Urząd nie musi przetwarzać danych, które są Urzędowi zbędne). Urząd może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Urząd procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.
8. Usunięcie danych – na żądanie osoby Urząd usuwa dane, gdy:
    a) dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,
    b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej ich przetwarzania,
    c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
    d) dane były przetwarzane niezgodnie z prawem,
    e) konieczność usunięcia wynika z obowiązku prawnego,
9. Ograniczenie przetwarzania – Urząd dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
    a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
    b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
    c) Urząd nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
    d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Urzędu zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
10. Sprzeciw w szczególnej sytuacji – jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Urząd w oparciu o uzasadniony interes Urzędu lub o powierzone Urzędowi zadanie w interesie publicznym, Urząd uwzględni sprzeciw, o ile nie zachodzą po stronie Urzędu ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
11. Wszystkie zagadnienia określone w § 12 ust. 1-10 analizuje IOD i przedstawia wnioski ADO wraz z projektem/propozycją ich rozstrzygnięcia.

§ 13

1. ADO zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych.
2. ADO we współpracy z IOD i ASI przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
    - zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych;
    - kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;
    - przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii;
    - analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o rożnym prawdopodobieństwie wystąpienia i wadze zagrożenia;
    - ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym ustala przydatność i stosuje takie środki i podejście, jak: pseudonimizacja, szyfrowanie danych osobowych, inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
3. ADO dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie. Organizacja stosuje metodykę oceny skutków przyjętą w Urzędzie.
4. ADO stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa i są bliżej opisane w procedurach dla tych obszarów.

§14

1. Urząd stosuje zasady doboru i weryfikacji podmiotów przetwarzających dane na rzecz Urzędu opracowane w celu zapewnienia, aby podmioty przetwarzające dawały wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Urzędzie.
2. Urząd rozlicza podmioty przetwarzające z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.
3. Urząd podpisuje umowę z podmiotem przetwarzającym dane, któremu powierzył przetwarzanie. Jej treść przed podpisaniem musi zostać pozytywnie zaopiniowana przez IOD.
4. IOD (realizując zadania na rzecz Urzędu) prowadzi rejestr umów powierzenia przetwarzania, którego wzór stanowi załącznik numer 6.

Załączniki do Polityki Bezpieczeństwa Informacji Urzędu Miasta w Kościerzynie:

1. Upoważnienie do przetwarzania danych osobowych - wzór.
2. Oświadczenie - wzór.
3. Ewidencja osób upoważnionych do przetwarzania danych osobowych - wzór.
4. Wykaz udostępnień danych osobowych innym podmiotom – wzór.
5. Wykaz pomieszczeń, w których przetwarzane są dane osobowe – wzór.
6. Rejestr umów powierzenia przetwarzania – wzór.
7. Rejestr analizy ryzyka – wzór.
8. Rejestr Czynności Przetwarzania Danych Osobowych (RCPD) – wzór.

Załącznik nr 1
do Polityki Bezpieczeństwa Informacji
Urzędu Miasta Kościerzyna

..... Kościerzyna, ...
(oznaczenie pracodawcy)

UPOWAŻNIENIE nr ….
do przetwarzania danych osobowych

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) (Dz.U.UE.L.2016.119.1) upoważniam Panią:

……
(imię i nazwisko pracownika)

zatrudnioną w Urzędzie Miasta Kościerzyna w **Wydziale ……** na stanowisku **……**, do przetwarzania danych osobowych zgodnie z przyjętą Polityką Bezpieczeństwa Informacji, Regulaminem Organizacyjnym Urzędu i stanowiskową kartą pracy oraz zobowiązuję Panią do przestrzegania zasad ochrony danych osobowych określonych w tych dokumentach.

1. Jednocześnie zobowiązuję Panią do zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobów ich zabezpieczenia.

2. Upoważnienie wygasa z chwilą rozwiązania umowy o pracę lub zmiany stanowiska pracy.

.....
podpis Administratora Danych Osobowych

Oświadczam, że zapoznałam się z przepisami dotyczącymi ochrony danych osobowych: 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 (Dz. Urz. UE L 119/1 z 4.5.2016 r.), ustawą z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U.2018.1000 z dnia 24 maja 2018r.) oraz przyjętą Polityką Bezpieczeństwa Informacji Urzędu Miasta Kościerzyna.

.....
Data i podpis pracownika

Załącznik nr 2
do Polityki Bezpieczeństwa Informacji
Urzędu Miasta Kościerzyna

OŚWIADCZENIE

1. Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam, lub będę miał/-a dostęp w związku z wykonywaniem jakichkolwiek czynności na rzecz Urzędu Miasta Kościerzyna i Gminy Miejskiej Kościerzyna. Zachowanie tajemnicy obowiązuje mnie także po zaprzestaniu tych czynności.

2. Zobowiązuję się chronić dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

3. Zobowiązuję się przestrzegać wszelkich procedur obowiązujących w wyżej wymienionej jednostce organizacyjnej dotyczących ochrony danych osobowych – w szczególności określonych w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym.

4. Oświadczam, że zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w tym z obowiązująca ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych oraz 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).

. . . . . .

(data i podpis osoby oświadczającej)

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Imię i nazwisko	Komórka organizacyjna	Zakres *(określenie, do jakich zbiorów dana osoba ma dostęp, zgodnie z załącznikiem numer 2 do Polityki Bezpieczeństwa)*	Data nadania upoważnienia	Data ustania upoważnienia	Identyfikator/Login w danym systemie informatycznym
1.						
2.						
3.						
4.						
5.						

Załącznik nr 4
do Polityki Bezpieczeństwa Informacji
Urzędu Miasta w Kościerzynie

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** *(np. upoważniony organ, instytucja lub inny, który wykazał uprawnienie do udostępnienia mu danych)*	**Cel udostępnienia** *(podstawa prawna/numer umowy)*	**Zakres udostępnionych danych** *(jakie dane zostały udostępnione)*	**Forma udostępnienia** *(np. papierowy wydruk, dane w formie elektronicznej)*
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						

Załącznik nr 5
do Polityki Bezpieczeństwa Informacji
Urzędu Miasta w Kościerzynie

WYKAZ POMIESZCZEŃ W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

wszystkie miejsca, pomieszczenia, pokoje, w których dokonuje się operacji na danych osobowych

L.p.	Lokalizacja – adres	Precyzyjne określenie pomieszczenia	Dział/osoba użytkująca pomieszczenie	Zabezpieczenie pomieszczenia
1	2	3	4	5
Budynek Urzędu Miasta w Kościerzynie, 83-400 Kościerzyna, ul. 3 Maja 9a				
1.				
2.				

Straż Miejska – Budynek przy ul Młyńskiej, 83-400 Kościerzyna, ul. Młyńska 15				
L.p.	**Lokalizacja-adres**	**Precyzyjne określenie pomieszczenia**	**Dział/osoba użytkująca pomieszczenie**	**Zabezpieczenie pomieszczenia**
1.				
2.				

Załącznik nr 6
do Polityki Bezpieczeństwa Informacji
Urzędu Miasta w Kościerzynie

Rejestr umów powierzenia przetwarzania

L.p.	Numer umowy / data zawarcia umowy / data wygaśnięcia umowy	Nazwa zbioru danych *(możliwie najpełniejszy opis osoby, której dane zostały udostępnione lub całego zbioru)*	Nazwa podmiotu, któremu udostępniono dane *(np. dane identyfikujące kontrahenta, nazwa firmy, NIP, adres siedziby, dane przedstawiciela)*	Cel udostępnienia *(podstawa prawna/numer umowy)*	Forma udostępnienia *(np. papierowy wydruk, dane w formie elektronicznej)*	Uwagi dodatkowe *(np. przedmiot umowy)*
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						

NAZWA JEDNOSTKI:	Urząd Miejski w Kościerzynie
TABELA I: FORMULARZ DO OBLICZANIA RYZYKA	aktualizacja rejestru:

Nr	IDENTYFIKACJA RYZYKA		ANALIZA RYZYKA							
			WAGA RYZYKA					Ujęcie procentowe [%]	Korekta wskaźnika	Wartość ryzyka w %
			Oddziaływanie ryzyka (O)				Prawdopodobieństwo wystąpienia ryzka (P)			
			Kryterium finansowe	Kryterium organizacyjne	Kryterium reputacji	Wpływ na Strategię				
			K_F	K_O	K_R	K_S	P	WR%	D	WK
	proces / zadanie / projekt	Nazwa ryzyka	0,4	0,2	0,2	0,2	(1-5)	(0%-100%)	+ / - 20% pkt.	(1 % - 100 %)
1	2	3	4	5	6	7	9	11	12	13
	Obliczanie ryzyka		lista wyboru	lista wyboru	lista wyboru	lista wyboru	lista wyboru	WR x 100% / 25 formuła	WR + / - D lista wyboru	WK formuła
1.										
2.										
3.										

Załącznik nr 8
do Polityki Bezpieczeństwa Informacji
Urzędu Miasta w Kościerzynie

REJESTR CZYNNOŚCI ORAZ REJEST KATEGORII CZYNNOŚCI PRZETWARZANIA

Lp.	Nazwa zbioru	Cel przetwarzania	Wykorzystane oprogramowanie / postać papierowa (okres przechowywania/ archiwizacji)	Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	Jednostka wykonująca	Kategorie osób	Źródło danych	Udostępnianie danych	Podstawa prawna	Informacja dot. transferu do kraju trzeciego poza UE	Techniczne i organizacyjne środki zabezpieczeń