

**ZARZĄDZENIE Nr 120/4/2019**

**Burmistrza Prudnika**

z dnia 12.03.2019 r.

**w sprawie wprowadzenia Polityki ochrony danych osobowych Urzędu Miejskiego w Prudniku**

Na podstawie art. 24 ust. 2 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. Urz. UE. L 119 z 04.05.2016, str. 1) zarządza się, co następuje:

**§ 1. 1.** W Urzędzie Miejskim w Prudniku, wprowadza się Politykę ochrony danych osobowych Urzędu Miejskiego w Prudniku, stanowiącą załącznik nr 1 do zarządzenia.

2. Określa się:

- 1) Wzór oświadczenia o zapoznaniu się z treścią Polityki ochrony danych osobowych, stanowiący załącznik nr 2 do zarządzenia;
- 2) Postępowanie w zakresie udzielania upoważnienia do przetwarzania danych osobowych, stanowiące załącznik nr 3 do zarządzenia;
- 3) Postępowanie dotyczące sporządzania rejestru czynności przetwarzania danych osobowych oraz rejestr kategorii przetwarzania danych osobowych, stanowiące załącznik nr 4 do zarządzenia;
- 4) Postępowanie w zakresie zawierania umów lub porozumień w sprawie powierzenia przetwarzania danych osobowych, stanowiące załącznik nr 5 do zarządzenia;
- 5) Wzór klauzuli informacyjnej w przypadku zbierania danych osobowych od osoby, której dane dotyczą, stanowiący załącznik nr 6 do zarządzenia;
- 6) Wzór klauzuli informacyjnej w przypadku zbierania danych osobowych w sposób inny niż od osoby, której dane dotyczą, stanowiący załącznik nr 7 do zarządzenia;
- 7) Postępowanie dotyczące wpłynięcia wniosku obywatela w zakresie przysługujących mu praw, stanowiące załącznik nr 8 do zarządzenia;
- 8) Wzór zgody na przetwarzanie danych osobowych, stanowiący załącznik nr 9 do zarządzenia;
- 9) Postępowanie w przypadku naruszenia ochrony danych osobowych, stanowiące załącznik nr 10 do zarządzenia.
- 10) Wzór rejestru nośników komputerowych zawierających ważne dane stanowiący załącznik nr 11 do zarządzenia

**§ 2.** Traci moc Zarządzenie Nr 69/2018 Burmistrza Prudnika z dnia 16 kwietnia 2018 r. w sprawie Polityki Ochrony Danych Osobowych w Urzędzie Miejskim w Prudniku

**§ 3.** Zarządzenie wchodzi w życie z dniem podjęcia.

**BURMISTRZ**  
Grzegorz Zawisłak

## **POLITYKA OCHRONY DANYCH OSOBOWYCH**

### **w Urzędzie Miejskim w Prudniku**

#### **ROZDZIAŁ I**

Podstawowe pojęcia:

- 1) Administrator – Burmistrz Prudnika, który decyduje o celach i sposobach przetwarzania danych osobowych;
- 2) KAG – Kierownik Referatu Administracyjno-Gospodarczego;
- 3) dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- 4) Inspektor Ochrony Danych (IOD) – pracownik Urzędu Miejskiego, który realizuje zadania określone w art. 39 RODO;
- 5) Burmistrz – Burmistrz Prudnika;
- 6) Urząd – Urząd Miejski w Prudniku ;
- 7) odbiorca – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, którym ujawnia się dane osobowe, niezależnie od tego, czy są stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców (przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania);
- 8) ograniczenie przetwarzania – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
- 9) organizacja międzynarodowa – organizacja i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy;
- 10) państwo trzecie – państwo niebędące członkiem Unii Europejskiej oraz nienależące do Europejskiego Obszaru Gospodarczego;

- 11) podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, którzy przetwarzają dane osobowe w imieniu administratora;
- 12) Polityka – Polityka ochrony danych osobowych;
- 13) profilowanie – dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
- 14) pseudonimizacja – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
- 15) 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);
- 16) strona trzecia – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które z upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe;
- 17) UODO – Urząd Ochrony Danych Osobowych – organ nadzorczy;
- 18) zgoda – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego przyzwala na przetwarzanie dotyczących jej danych osobowych;

## **ROZDZIAŁ II Postanowienia ogólne**

§ 1. 1. Polityka ma zastosowanie do przetwarzania danych osobowych w Urzędzie , w szczególności w związku z realizacją:

- 1) zadań wynikających z przepisów prawa oraz zadań określonych w Regulaminie Organizacyjnym Urzędu;
- 2) obowiązków pracodawcy w rozumieniu Kodeksu pracy;
- 3) umów o organizację staży, praktyk, wolontariatu;
- 4) innych zadań niezbędnych do zapewnienia funkcjonowania Urzędu.

2. W Urzędzie dane osobowe przetwarzane są co do zasady na podstawie następujących przesłanek:

1) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

2) przetwarzanie jest niezbędne do wypełniania obowiązku prawnego ciążącego na administratorze.

3) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

4) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora.

3. Dane osobowe mogą być przetwarzane w Urzędzie w postaci papierowej oraz przy użyciu systemów informatycznych, które zostały wskazane w Instrukcji Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych.

### **ROZDZIAŁ III Ogólne zasady przetwarzania danych osobowych**

§ 2. 1. Przetwarzanie danych osobowych w Urzędzie oznacza każdą operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, tj.:

1) zbieranie;

2) utrwalanie;

3) organizowanie;

4) porządkowanie;

5) przechowywanie;

6) adaptowanie lub modyfikowanie;

7) pobieranie;

8) przeglądanie;

9) wykorzystywanie;

10) ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie;

11) dopasowywanie lub łączenie;

12) ograniczanie;

13) usuwanie lub niszczenie.

2. Zbieranie danych osobowych należy rozumieć jako pozyskiwanie danych osobowych.

3. Za utrwalanie należy przyjąć wszelkie formy i postaci zarejestrowania (zapisania) informacji na materialnym nośniku – informacja utrwalona, co do zasady, nadawać się powinna do dalszego przetwarzania zgodnie z celem, w jakim ją zebrano.

4. Organizowanie danych to operacje nieodnoszące się do zmiany treści lub postaci przechowania samych danych, a polegające na nadaniu określonej struktury zbiorowi czy zestawowi, w jakim dane są przetwarzane, lub zmianie jego dotychczasowej struktury.

5. Porządkowanie to operacja, która ma poprawić funkcjonalność użytkowania danych, w szczególności poprzez wprowadzenie jakichkolwiek lub lepszych niż dotychczasowe kryteriów wyszukiwania dostępu do określonych kategorii informacji.

6. Operacja przechowania jest związana z uprzednim utwaleniem danych osobowych na nośniku materialnym z możliwością ich odtworzenia w późniejszym czasie.

7. Adaptowanie lub modyfikowanie danych osobowych polega na uzyskaniu nowej wiedzy na temat osoby, której dane są przetwarzane. Adaptowanie danych osobowych jest zmianą wynikającą ze skorzystania przez osobę, której dane są przetwarzane, z przysługujących jej praw, w szczególności: ograniczenia przetwarzania, usunięcia części danych. Modyfikacja danych związana jest z ingerencją osoby, której dane dotyczą, tj. sprostowania danych.

8. Pobieranie danych osobowych jest operacją związaną z wykonywaniem kopii danych osobowych lub ich części pozyskanych za pośrednictwem sieci telekomunikacyjnej lub innego kanału przesyłu informacji.

9. Przeglądanie danych należy rozumieć jako wyszukiwanie danych poprzez wpisywanie odpowiednich haseł, które dzięki zastosowanemu mechanizmowi indeksującemu pozwalają na zapoznanie się z konkretnymi danymi.

10. Wykorzystywanie danych jest celowym działaniem zmierzającym do konkretnego celu.

11. Ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie należy rozumieć jako operacje, które prowadzą do zapoznania się z danymi przez podmioty zewnętrzne za zgodą administratora.

12. Dopasowywanie lub łączenie danych osobowych polega na aktywnym działaniu podjętym przez administratora w celu weryfikacji poprawności danych, uzyskanie dodatkowych informacji wynikających ze skali przetwarzania czy usprawnienie procesów przetwarzania.

13. Ograniczenie oznacza każdą formę zawężenia możliwości przetwarzania. Dotyczy to zarówno zakresu przetwarzanych informacji, jak i celów dla jakich są one wykorzystywane.

14. Usuwanie lub niszczenie polega na trwałym kasowaniu danych.

§ 3. 1. Administrator przetwarza dane osobowe zgodnie z następującymi zasadami:

- 1) legalności;
- 2) rzetelności;
- 3) przejrzystości;
- 4) ograniczenia celu;
- 5) minimalizacji danych;

- 6) prawidłowości danych;
- 7) ograniczenia przechowywania;
- 8) integralności i poufności;
- 9) ochrony danych osobowych w fazie projektowania;
- 10) domyślnej ochrony danych osobowych.

2. Zasada legalności oznacza przetwarzanie danych zgodnie z prawem. Realizując tę zasadę, dane osobowe przetwarzane są na podstawie co najmniej jednej z przesłanek przetwarzania danych osobowych.

3. Zasada rzetelności wymaga, by dane były przetwarzane z uwzględnieniem interesów i uzasadnionych oczekiwań osób, których dane dotyczą.

4. Zasada przejrzystości wymaga by osoba, której dane dotyczą została należycie poinformowana o istotnych dla niej aspektach tego przetwarzania, tj. w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

5. Zasada ograniczenia celu polega na przetwarzaniu danych osobowych jedynie w celu zgodnym z odpowiednią przesłanką dopuszczalności przetwarzania danych osobowych.

6. Zasada minimalizacji danych oznacza, że administrator przetwarza tylko te dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania.

7. Zasada prawidłowości danych oznacza, że administrator przetwarza dane osobowe prawidłowe i uaktualnia je w razie potrzeby.

8. Zasada ograniczenia przechowywania oznacza, że administrator przechowuje dane osobowe w dokumentacji tworzącej akta spraw przez okres wynikający z Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.

9. Zasada integralności i poufności jest realizowana przez dopuszczenie do przetwarzania danych osobowych jedynie osób upoważnionych oraz zastosowanie takich środków technicznych i organizacyjnych, by dane nie były zmieniane przez osoby nieupoważnione lub by dane nie były udostępniane osobom nieupoważnionym.

10. Zasada ochrony danych osobowych w fazie projektowania oznacza, że ochrona prywatności jest realizowana na etapie projektowanych działań skutkujących przetwarzaniem danych osobowych.

11. Zasada domyślnej ochrony danych osobowych oznacza, że domyślne ustawienia przetwarzania danych osobowych umożliwią przetwarzanie jedynie danych niezbędnych do osiągnięcia każdego konkretnego celu przetwarzania. Jednocześnie ustawienia systemów przetwarzania danych nie powinny umożliwiać udostępnienia danych nieokreślonej liczbie osób fizycznych bez interwencji osoby, której dane dotyczą.

## **ROZDZIAŁ IV Wydawanie upoważnień do przetwarzania danych osobowych**

§ 4. 1. W Urzędzie przetwarzanie danych osobowych odbywa się na podstawie upoważnień.

2. Upoważnienie wydawane jest osobie, która:

- 1) w ramach obowiązków służbowych przetwarza dane osobowe;
- 2) złożyła oświadczenie o zachowaniu poufności;
- 3) została przeszkolona w zakresie ochrony danych osobowych przez IOD.

3. Sposób wydawania upoważnień do przetwarzania danych osobowych określa załącznik nr 3 do zarządzenia.

4. Osoba upoważniona do przetwarzania danych osobowych jest obowiązana do:

- 1) zapoznania się z obowiązującymi przepisami prawa dotyczącymi ochrony danych osobowych;
- 2) przechodzenia okresowych szkoleń z obszaru ochrony danych osobowych;
- 3) stosowania określonych w Urzędzie procedur i środków przetwarzania;
- 4) zabezpieczenia danych osobowych przed ich utratą, uszkodzeniem lub zniszczeniem, zmianą lub udostępnieniem osobom nieupoważnionym;
- 5) przestrzegania procedur właściwego użytkowania systemów informatycznych, w których przetwarza się dane osobowe, w tym do nieujawniania innym użytkownikom swoich loginów i haseł;
- 6) nieopuszczania stanowiska bez zabezpieczenia dokumentów papierowych, zawierających dane osobowe oraz bez zabezpieczania dostępu do danych osobowych przetwarzanych w systemie informatycznym;
- 7) zaprzestania przetwarzania danych osobowych po ustaniu stosunku zatrudnienia.

## **ROZDZIAŁ V Rejestr czynności przetwarzania danych oraz rejestr kategorii czynności przetwarzania danych**

§ 5.1. W Urzędzie prowadzi się rejestr czynności przetwarzania danych oraz rejestr kategorii czynności przetwarzania danych.

2. Rejestr czynności przetwarzania danych i rejestr kategorii czynności przetwarzania danych dla Urzędu może być udostępniany UODO na każde jego wezwanie.

3. Sposób tworzenia rejestru czynności przetwarzania danych oraz rejestru kategorii czynności przetwarzania danych określa załącznik nr 4 do zarządzenia.

## **ROZDZIAŁ VI Umowy lub porozumienia w sprawie powierzenia przetwarzania danych osobowych**

§ 6. Zadania skutkujące powierzeniem przetwarzania danych osobowych innemu podmiotowi, powierza się podmiotowi, który zapewni wystarczającą gwarancję wdrożenia odpowiednich

środków technicznych i organizacyjnych, by przetwarzanie chroniło prawa osób, których dane dotyczą.

2. Przyjęcie powierzenia przetwarzania danych wymaga zgody administratora.

3. Szczegółowy sposób postępowania w zakresie wskazanym w ust. 1 i 2 określa załącznik nr 5 do zarządzenia.

## **ROZDZIAŁ VII Prawa osób, których dane są przetwarzane w Urzędzie, niewymagające wniosku obywatela oraz sposób ich realizacji**

§ 7. 1. Podstawowym prawem osoby, której dane są przetwarzane w Urzędzie, jest bycie poinformowanym o fakcie przetwarzania danych osobowych.

2. Zakres realizacji prawa wskazanego w ust. 1 zależy od sposobu pozyskania danych osobowych, tj. bezpośrednio od osoby, której dane dotyczą, lub w sposób inny niż od osoby, której dane dotyczą.

§ 8.1. W przypadku zbierania danych od osoby, której dane dotyczą, administrator w momencie pozyskiwania danych ma obowiązek przekazać w szczególności następujące informacje o:

- 1) tożsamości administratora danych;
- 2) celach przetwarzania danych;
- 3) przysługujących prawach osobie, której dane są przetwarzane.

2. Przepis ust. 1 nie stosuje się, gdy i w zakresie w jakim osoba, której dane dotyczą, dysponuje już tymi informacjami.

3. Ramowy zakres klauzuli informacyjnej w przypadku zbierania danych od osoby, której dane dotyczą, określa załącznik nr 6 do zarządzenia.

§ 9.1. W przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą, Administrator podaje osobie, której dane dotyczą w szczególności następujące informacje o:

- 1) tożsamości administratora danych;
- 2) celach przetwarzania danych;
- 3) przysługujących prawach osobie, które dane są przetwarzane;
- 4) od kogo otrzymał dane osobowe.

2. Informacje, o których mowa w ust. 1, podaje się najpóźniej:

- 1) nie później niż w terminie miesiąca od momentu pozyskania danych osobowych lub
- 2) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – przy pierwszej takiej komunikacji z tą osobą lub
- 3) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – przy ich pierwszym ujawnieniu.

3. Obowiązku, o którym mowa w ust. 1, nie stosuje się gdy i w zakresie w jakim:

- 1) osoba, której dane dotyczą, dysponuje już tymi informacjami;



2)udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, w szczególności w przypadku przetwarzania danych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń odpowiednich dla tych danych, lub o ile obowiązek, o którym mowa w ust. 1, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania; w takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;

3)pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii Europejskiej lub prawem krajowym przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą;

4)dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii Europejskiej lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

4.Ramowy zakres klauzuli informacyjnej w przypadku zbierania danych w sposób inny niż od osoby, której dane dotyczą, określa załącznik nr 7 do zarządzenia.

§ 10.1.Za realizację obowiązku informacyjnego, o którym mowa w § 8 i 9, odpowiedzialni są Kierownicy komórek organizacyjnych, w których dane osobowe danej osoby będą przetwarzane.

2.Informacje, o których mowa w § 8 i 9, mogą zostać przekazane na piśmie, w tym elektronicznie, a w szczególnych przypadkach mogą zostać odczytane.

3.Każdorazowo należy udokumentować przekazanie informacji, o których mowa w § 8 i 9.

4.Istnieje możliwość konsultowania sposobu realizowania obowiązków, o których mowa w § 8 i 9 z IOD.

## **ROZDZIAŁ VIII Prawa obywateli, których dane są przetwarzane w Urzędzie, wymagające wniosku**

§ 11. 1.Obywatelowi, którego dane są przetwarzane, przysługuje prawo:

1)dostępu do danych przetwarzanych w Urzędzie oraz uzyskania potwierdzenia, czy Urząd przetwarza jego dane;

2)prostowania dotyczących go danych osobowych, które są nieprawidłowe, z uwzględnieniem celów przetwarzania;

3)do usunięcia danych (tzw. prawo do bycia zapomnianym);

4)do ograniczenia przetwarzania ;

5)do przenoszenia danych;

6)do sprzeciwu wobec przetwarzania dotyczących jej danych osobowych.

2.Realizacja praw, o których mowa w ust. 1, odbywa się na podstawie pisemnego wniosku obywatela, którego dane dotyczą.

3.Sposób realizacji praw obywatela, którego dane dotyczą, wymagających wniosku określa załącznik nr 8 do zarządzenia.

## **ROZDZIAŁ IX Przetwarzanie danych osobowych na podstawie zgody osoby, której dane są przetwarzane w Urzędzie**

§ 12.1.W szczególnych przypadkach przewidzianych prawem lub w sytuacjach, gdy przetwarzanie jest wymagane dla prawidłowej realizacji zadania, a nie mają zastosowania przesłanki wskazane w § 1 ust. 2, przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą.

2.W celu realizacji zasady rozliczalności zgoda powinna być udokumentowana w formie pisemnej.

3.Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy również innych kwestii, oświadczenie zgody musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii.

4.Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

5.Ramowy wzór treści zgody określa załącznik nr 9 do zarządzenia.

## **ROZDZIAŁ X Udostępnianie danych osobowych**

§ 13. 1.Udostępnianie danych osobowych przez Urząd wynika jedynie z obowiązujących przepisów prawa.

2.Pracownicy komórek organizacyjnych, do których wpływają wnioski o udostępnienie danych, obowiązani są każdorazowo do przeanalizowania możliwości oraz zakresu udostępnienia danych osobowych w uzgodnieniu z IOD.

3.W celu zapewnienia przez Urząd kontroli nad tym, komu dane są przekazywane, udostępnienie danych powinno odbywać się co do zasady w formie pisemnej, co pozwoli w szczególności na udokumentowanie podstawy prawnej udostępnienia danych i podmiotu, który o to się zwróci.

## **ROZDZIAŁ XI Przekazanie danych osobowych do państw trzecich**

§ 14.1.Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych może odbywać jedynie zgodnie z zasadami wskazanymi w rozdziale V RODO.

2.Kierownicy komórek organizacyjnych Urzędu obowiązani są zweryfikować istnienie podstawy prawnej uprawniającej do przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej przed dokonaniem przekazania.

3.Przekazanie danych osobowych odbywa się tylko w formie pisemnej.

## **ROZDZIAŁ XII Naruszenia ochrony danych osobowych**

§ 15.1. Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:

- 1) zniszczenia lub
- 2) utracenia, lub
- 3) zmodyfikowania, lub
- 4) nieuprawnionego ujawnienia, lub
- 5) nieuprawnionego dostępu

2. Pracownicy Urzędu obowiązani są zgłaszać każde zdarzenie zagrażające bezpieczeństwu, a ustalenie czy stanowi ono naruszenie ochrony danych osobowych należy do IOD.

3. Sposób postępowania w przypadku naruszeń ochrony danych osobowych oraz ich zgłaszanie i dokumentowanie określa załącznik nr 10 do zarządzenia .

## **ROZDZIAŁ XIII Przeprowadzenie oceny skutków dla ochrony danych osobowych**

§ 16.1. Ocenę skutków dla ochrony danych osobowych planowanych procesów przetwarzania przeprowadza się, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.

2. Ocena skutków dla ochrony danych osobowych przeprowadzana jest przez komórkę organizacyjną Urzędu, w której będzie odbywało się lub odbywa się przetwarzanie danych osobowych wymagające przeprowadzenia oceny skutków dla ochrony danych osobowych.

3. Komórka organizacyjna realizująca proces wskazany w ust. 1 jest obowiązana skonsultować z IOD w szczególności kwestie dotyczące:

- 1) faktu, czy należy przeprowadzić ocenę skutków dla ochrony danych osobowych;
- 2) metodologii przeprowadzenia oceny skutków dla ochrony danych osobowych;
- 3) zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń naruszenia praw i wolności osób, których dane dotyczą;
- 4) prawidłowości przeprowadzonej oceny skutków dla ochrony danych osobowych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie, czy też nie oraz jakie zabezpieczenia należy stosować).

4. Za przeprowadzenie oceny skutków dla ochrony danych osobowych odpowiedzialni są Kierownicy komórek organizacyjnych Urzędu.

5. W stosownych przypadkach Kierownik komórki organizacyjnej, który odpowiada za daną operację przetwarzania danych, zasięga opinii osób, których dane dotyczą, lub ich

przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania.

§ 17.1. Ocena skutków dla ochrony danych osobowych zawiera co najmniej następujące elementy:

- 1) opis planowanych operacji przetwarzania i celów przetwarzania, w tym gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez Urząd;
- 2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
- 3) ocenę ryzyka naruszenia praw lub wolności obywateli, których dane dotyczą;
- 4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

2. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z procesu przetwarzania, Kierownik komórki organizacyjnej Urzędu, który odpowiada za dany proces, dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych osobowych.

3. W sytuacji o której mowa w ust. 2 Kierownik komórki organizacyjnej Urzędu sporządza notatkę, która zawiera w szczególności elementy wskazane w ust. 1 po uwzględnieniu zmian.

4. Kierownik komórki organizacyjnej Urzędu po sporządzeniu notatki, o której mowa w ust. 3, jest obowiązany do przekazania jej IOD.

§ 18.1. Oceny skutków dla ochrony danych osobowych nie przeprowadza się, jeżeli

przetwarzanie odbywa się na podstawie przesłanki wskazanej w § 1 ust. 2 pkt 2 i 3 oraz gdy spełniono łącznie poniższe warunki:

- 1) ma podstawę prawną w prawie Unii Europejskiej lub w prawie polskim i prawo takie reguluje daną operację przetwarzania lub zestaw operacji;

- 2) oceny skutków dla ochrony danych osobowych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej.

§ 19. Jeżeli przeprowadzona ocena skutków dla ochrony danych osobowych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, przed rozpoczęciem przetwarzania Administrator konsultuje się z organem nadzorczym.

## ROZDZIAŁ XIV Inspektor Ochrony Danych (IOD)

§ 20.1. IOD posiada kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności niezbędne do wypełnienia następujących zadań:

- 1) informowania Administratora oraz pracowników Urzędu (w tym stażystów, praktykantów, wolontariuszy, osób wypełniających zadania w ramach umów cywilnoprawnych) o obowiązkach spoczywających na nich z mocy RODO oraz wynikających z innych przepisów w zakresie ochrony danych osobowych;
- 2) doradzania Burmistrzowi oraz pracownikom Urzędu (w tym stażystom, praktykantom, wolontariuszom, osobom wypełniającym zadania w ramach umów cywilnoprawnych) w zakresie obowiązków spoczywających na nich z mocy RODO oraz innych przepisów w zakresie ochrony danych osobowych;
- 3) monitorowania przestrzegania RODO oraz innych przepisów o ochronie danych osobowych, polityk ochrony danych osobowych wdrożonych w Urzędzie;
- 4) udzielania zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorowania wykonania oceny skutków dla ochrony danych osobowych;
- 5) współpracy z UODO i pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenia konsultacji we wszystkich innych sprawach;
- 6) pełnienia roli punktu kontaktowego dla osób, których dane dotyczą.

2. IOD może wykonywać inne zadania i obowiązki niż wskazane w ust. 1.

3. IOD funkcjonuje w ramach Wydziału Organizacyjnego Urzędu.

4. IOD podlega bezpośrednio Burmistrzowi, któremu składa roczne sprawozdanie w zakresie podejmowanych działań.

5. IOD ma zapewniony dostęp do zasobów lokalowych, materialnych i finansowych niezbędnych do wykonywania powierzonych zadań

6. IOD ma zapewniony dostęp do zasobów niezbędnych do utrzymania jego wiedzy fachowej (szkolenia, kursy, warsztaty, prasa, publikacje).

§ 21. 1. IOD wypełnia swoje zadania z należyтым uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

2. W ramach wykonywania zadań IOD obowiązany jest do ustalania priorytetów w swojej pracy i koncentrowania się na aspektach pociągających za sobą większe ryzyko w zakresie ochrony danych osobowych.

3. IOD jest obowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego.

4.Kierownicy komórek organizacyjnych obowiązani są do informowania IOD:

1)o wszystkich istniejących i planowanych procesach przetwarzania danych oraz konsultowania z IOD tych kwestii, przy czym niezbędne informacje powinny być przekazywane IOD odpowiednio wcześniej, umożliwiając mu zajęcie stanowiska;

2)o każdym spotkaniu podczas którego będą omawiane sprawy związane z ochroną danych osobowych.

§ 22. 1.Zadanie dotyczące informowania Administratora oraz pracowników Urzędu o obowiązkach spoczywających na nich w ramach ochrony danych osobowych IOD wykonuje w szczególności poprzez:

1)przeprowadzenie szkolenia wstępnego przed rozpoczęciem przez pracowników (w tym stażystów, praktykantów, wolontariuszy, osoby wypełniające zadania w ramach umów cywilnoprawnych) służbowych obowiązków;

2)prorowadzenie lub organizowanie cyklicznych wykładów, szkoleń, warsztatów;

3)przekazywanie materiałów informacyjnych;

4)udział w opracowywaniu regulaminów lub procedur związanych z przetwarzaniem danych.

2.Doradzanie Burmistrzowi oraz pracownikom Urzędu w zakresie obowiązków spoczywających na nich z mocy RODO oraz innych przepisów w zakresie ochrony danych osobowych IOD realizuje poprzez przygotowywanie opinii, notatek służbowych, udział w ocenie skutków dla ochrony danych osobowych.

3.Monitorowanie przestrzegania obowiązujących przepisów związanych z ochroną danych osobowych oraz procedur wewnętrznych IOD realizuje w szczególności poprzez przeprowadzanie czynności monitoringowych, w ramach których zbiera informacje w celu identyfikacji czynności przetwarzania oraz przeprowadza analizę zgodności tego przetwarzania.

4.W ramach współpracy z organem nadzorczym i pełnieniem funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem IOD:

1)przygotowuje, we współpracy z innymi komórkami organizacyjnymi, odpowiedzi na pisma i zapytania organu nadzorczego;

2)kontaktuje się w celu uzyskania porady ze strony organu nadzorczego.

5.Szczegółowe zadania realizowane w ramach pełnienia przez IOD punktu kontaktowego dla osób, których dane dotyczą, zostały opisane w rozdziale

## **VIII. ROZDZIAŁ XV Środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych przetwarzanych w Urzędzie**

§ 23.1.Środki techniczne i organizacyjne w systemach informatycznych stosowane w celu zapewnienia bezpieczeństwa danych osobowych przetwarzanych w Urzędzie są określone w Polityce Bezpieczeństwa Informacji w obszarze IT.

2.Środki techniczne i organizacyjne dotyczące fizycznego dostępu do obszaru, w którym przetwarzane są dane osobowe, są określone w regulacjach wewnętrznych Urzędu.

3.Środki techniczne i organizacyjne, o których mowa w ust. 1 i 2, zostały dobrane na podstawie przeprowadzonej analizy ryzyka, w której uwzględniono następujące elementy:

1)stan wiedzy technicznej;

2)koszt wdrożenia środków technicznych i organizacyjnych;

3)charakter przetwarzania, przez który należy rozumieć sposób dokonywania przetwarzania, w tym częstotliwość, czasowość, długoterminowość, masowość;

4)zakres przetwarzania (katalog operacji na danych osobowych);

5)kontekst przetwarzania, czyli kategorie przetwarzanych danych, kategorie osób, których dane dotyczą, okoliczności zbierania i dalszego przetwarzania, otoczenie i zagrożenia dla bezpieczeństwa i integralności danych;

6)cele przetwarzania.

4.Analiza ryzyka przeprowadzana jest raz w roku i w szczególnie uzasadnionych przypadkach (w szczególności w związku z dodatkowymi zadaniami Urzędu czy w związku z wystąpieniem naruszenia) poddawana przeglądowi pod kątem jej aktualności.

5.Sposób przeprowadzania i dokumentowania wyników analizy ryzyka opisują odrębne regulacje obowiązujące w Urzędzie.

## **ROZDZIAŁ XVI Odpowiedzialność za przetwarzanie danych osobowych**

§ 24. 1.Kierownicy komórek organizacyjnych są odpowiedzialni za zarządzanie procesami przetwarzania danych osobowych w swoich komórkach.

2.Każdy pracownik Urzędu jest obowiązany przestrzegać postanowień niniejszej Polityki.

3.Za nieprzestrzeganie niniejszej Polityki pracownik ponosi odpowiedzialność na zasadach określonych w przepisach prawa.

Wzór

Prudnik, dnia ..... / ..... / .....

.....  
Komórka organizacyjna

.....  
Imię i nazwisko

**OŚWIADCZENIE O ZAPOZNANIU SIĘ Z TREŚCIĄ POLITYKI OCHRONY  
DANYCH OSOBOWYCH OBOWIĄZUJĄCĄ W URZĘDZIE**

Oświadczam, że zapoznałam(-łem) się z treścią Polityki ochrony danych osobowych i zobowiązuję się do przestrzegania zawartych w tym dokumencie zasad, reguł i postanowień.

\_\_\_\_\_  
Data i podpis



### **Postępowanie w zakresie udzielenia upoważnienia do przetwarzania danych osobowych**

CEL PROCEDURY Przedstawienie wzoru upoważnienia do przetwarzania danych osobowych przetwarzanych w Urzędzie.

#### **ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY**

1. KAG – w ustalonym zakresie przygotowania i gromadzenia upoważnień do przetwarzania danych osobowych.

2. Kierownicy komórek organizacyjnych Urzędu – w zakresie występowania z wnioskiem o nadanie upoważnień do przetwarzania danych osobowych dla podległych pracowników oraz innych osób im podległych (stażystów, praktykantów, wolontariuszy oraz osób realizujących zadania na podstawie umowy cywilnoprawnej na rzecz danej komórki organizacyjnej)

#### **POSTANOWIENIA OGÓLNE**

1. KAG przygotowuje upoważnienia do przetwarzania danych osobowych dla pracowników Urzędu oraz innych osób, w szczególności stażystów, praktykantów, wolontariuszy oraz osób realizujących zadania na podstawie umowy cywilnoprawnej na rzecz danej komórki organizacyjnej, jeżeli realizowane przez nich zadania wiążą się z przetwarzaniem danych osobowych w Urzędzie.

2. Upoważnienia podpisywane są przez administratora.

#### **POSTANOWIENIA SZCZEGÓŁOWE PROCEDURY**

1. Kierownik komórki organizacyjnej występuje z wnioskiem o wydanie upoważnienia do przetwarzania danych osobowych dla pracowników oraz innych osób mu podległych (stażystów, praktykantów, wolontariuszy oraz osób realizujących zadania na podstawie umowy cywilnoprawnej na rzecz danej komórki organizacyjnej) w związku z:

- 1) podjęciem pracy w Urzędzie,
- 2) zmianą zakresu obowiązków,
- 3) zmianą stanowiska pracy lub komórki organizacyjnej Urzędu,
- 4) organizacją stażu lub praktyki lub wolontariatu,
- 5) realizacją umowy cywilnoprawnej – jeżeli realizowane przez nich zadania wiążą się z przetwarzaniem danych osobowych w Urzędzie.

2. Wzór wniosku znajduje się w niniejszej procedurze.

3. Upoważnienie do przetwarzania danych osobowych może być w każdym czasie odwołane przez administratora na wniosek KAG, IOD lub Kierownika komórki organizacyjnej, wskazanej w ust 1.

4.KAG prowadzi „Ewidencję osób upoważnionych w Urzędzie do przetwarzania danych osobowych”, w której w szczególności odnotowuje się następujące informacje:

1)imię i nazwisko upoważnionego;

2)komórka organizacyjna;

3)status osoby (pracownik, stażysta, praktykant, wolontariusz, umowa cywilnoprawna); 4)data wydania upoważnienia;

5)data ustania upoważnienia;

6)wskazanie procesu przetwarzania danych osobowych, w którym upoważniony będzie uczestniczył (z rejestru czynności przetwarzania danych osobowych).

5.Mogą być prowadzone dodatkowe ewidencje osób upoważnionych do przetwarzania danych w sytuacji, gdy wynika to z zawartej umowy lub porozumienia w sprawie powierzenia przetwarzania danych osobowych.

## Wzór

### Wniosek o wydanie upoważnienia do przetwarzania danych osobowych

1. Wniosek o wydanie upoważnienia dla:

Lp.	Imię i nazwisko	Stanowisko / status (stażysta / praktykant/ wolontariusz / realizacja umowy cywilnoprawnej)	Komórka organizacyjna	Okres obowiązania

2. Wnioskuje o wydanie upoważnienia do przetwarzania danych osobowych w związku z<sup>1</sup>:

- 1) aktualizacją posiadanego upoważnienia do przetwarzania danych osobowych;
- 2) podjęciem pracy w Urzędzie;
- 3) zmianą zakresu obowiązków;
- 4) zmianą stanowiska pracy lub komórki organizacyjnej;
- 5) zawarciem umowy cywilnoprawnej nr ..... z dnia .....
- 6) organizacją stażu/praktyki/wolontariatu<sup>1</sup>.

3. Przetwarzanie danych odbywać się będzie w postaci papierowej i elektronicznej. Główne systemy informatyczne, w których następuje przetwarzanie danych to:

- 1).....
- 2).....
- 3).....

4. Dane osobowe będą przetwarzane w ramach następujących procesów (zgodnie z rejestrem czynności właściwym dla danej komórki organizacyjnej)

- 1).....
- 2).....

5. Okres na jaki ma być udzielone upoważnienie<sup>1</sup>:

- 1) na czas trwania stosunku pracy (umowy z kodeksu pracy,);
- 2) do dnia..... (w przypadku pozostałych osób, które będą przetwarzały dane osobowe w imieniu administratora),

6. Kategorie danych, które będą przetwarzane :

- 1) zwykłe;
- 2) szczególne<sup>2</sup>

.....

<sup>1</sup> niewłaściwe usunąć

<sup>2</sup> dane szczególne to w szczególności: informacje o stanie zdrowia, przynależności do związków zawodowych, biometria, informacje o orientacji seksualnej, pochodzeniu etnicznym.

Prudnik, dnia .... / .... / .....

Nr upoważnienia .....

## UPOWAŻNIENIE 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. Urz. UE L 119 z 04.05.2016) upoważniam: Panią/Pana ..... zatrudnioną(-nego), odbywającą(-cego) staż, realizującą(-cego) praktykę lub wolontariat na stanowisku ..... w Wydziale ..... w Urzędzie Miejskim w Prudniku do przetwarzania danych osobowych w celach związanych z realizacją: •zadań służbowych powierzonych przez przełożonego lub w opisie stanowiska pracy<sup>1</sup> lub w zakresie obowiązków<sup>1</sup> oraz wynikających z realizacji czynności wskazanych w rejestrze czynności przetwarzania danych ..... (wskazać cel przetwarzania zgodnie z rejestrem czynności), lub •programu stażu, praktyki lub wolontariatu oraz wynikających z realizacji czynności wskazanych w rejestrze czynności przetwarzania danych właściwego ..... (wskazać cel przetwarzania zgodnie z rejestrem czynności).

Upoważnienie obejmuje przetwarzanie danych osobowych zlokalizowanych w systemach tradycyjnych: w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych, w związku z realizacją powierzonych obowiązków pracowniczych oraz w funkcjonujących systemach informatycznych, w zakresie niezbędnym do wykonywania obowiązków na ww. stanowisku:

1.....

2.....

Upoważnienie obejmuje przetwarzanie danych<sup>1</sup>:

1)zwykłych

2)szczególnych

Upoważnienie ważne jest od dnia ..... do dnia jego odwołania lub ustania Pani/Pana stosunku pracy, zakończenia stażu lub praktyki/wolontariatu<sup>1</sup>.

.....  
Podpis Administratora

<sup>1</sup>niewłaściwe usunąć.

Wzór - Oświadczenie osoby upoważnionej

1.Zobowiązuję się do przetwarzania danych osobowych zgodnie z powszechnie obowiązującymi przepisami prawa, w szczególności 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).

2.Oświadczam, że znane mi są przepisy dotyczące ochrony danych osobowych.

3.Zobowiązuję się do zapewnienia ochrony przetwarzanych danych osobowych, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnieniem, zabraniem, uszkodzeniem oraz modyfikacją lub zniszczeniem. Zobowiązuję się do natychmiastowego zgłaszania zaobserwowanej próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa danych lub systemu informatycznego Inspektorowi Ochrony Danych.

4.Zobowiązuję się do zachowania poufności i nieujawniania osobom trzecim informacji dotyczących przetwarzanych danych.

5.Zobowiązuję się do nierozpowszechniania i niewykorzystywania poufnych informacji zdobytych w trakcie wykonywania powierzonych prac, w szczególności informacji dotyczących funkcjonowania systemów służących do przetwarzania danych osobowych, do których zostałam(-łem) upoważniona(-ny) oraz haseł i zasad dostępu do tych systemów także po ustaniu umowy wiążącej mnie z Urzędem. Z chwilą ustania umowy zobowiązuję się do niezwłocznego zwrócenia wszelkich dokumentów oraz innych materiałów dotyczących danych osobowych.

6.Przyjmuję do wiadomości, że przetwarzanie danych osobowych z naruszeniem udzielonego upoważnienia może skutkować poniesieniem odpowiedzialności karnej.

---

Data i podpis Upoważnionego

Wzór

Nr upoważnienia .....

Prudnik, dnia ... / ... / .....

**UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH NA  
PODSTAWIE UMOWY CYWILNOPRAWNEJ**

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. Urz. UE L 119 z 04.05.2016, str.

1) upoważniam: Panią/Pana .....  
do przetwarzania danych osobowych w celach związanych z realizacją umowy cywilnoprawnej nr ..... Upoważnienie obejmuje przetwarzanie danych osobowych zlokalizowanych w systemach tradycyjnych: w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych, w związku z realizacją wyżej wskazanej umowy oraz w funkcjonujących systemach informatycznych w zakresie niezbędnym do wykonywania wyżej wskazanej umowy:

- 1).....
- 2).....
- 3).....

Upoważnienie obejmuje przetwarzanie danych<sup>1</sup>:

- 1) zwykłych
- 2) szczególnych

Upoważnienie ważne jest od dnia ..... do dnia jego odwołania lub wygaśnięcia umowy.

.....  
Podpis Administratora

<sup>1</sup> niewłaściwe usunąć.

### **Oświadczenie w związku z realizacją umowy cywilnoprawnej**

1. Zobowiązuję się do przetwarzania danych osobowych zgodnie z powszechnie obowiązującymi przepisami prawa, w szczególności 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).

2. Oświadczam, że znane mi są przepisy dotyczące ochrony danych osobowych.

3. Zobowiązuję się do zapewnienia ochrony przetwarzanych danych osobowych, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnieniem, zabranieniem, uszkodzeniem oraz modyfikacją lub zniszczeniem. Zobowiązuję się do natychmiastowego zgłaszania zaobserwowanej próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa danych lub systemu informatycznego Inspektorowi Ochrony Danych.

4. Zobowiązuję się do zachowania poufności i nieujawniania osobom trzecim informacji dotyczących przetwarzanych danych osobowych.

5. Zobowiązuję się do nierozpowszechniania i niewykorzystywania poufnych informacji zdobytych w trakcie wykonywania powierzonych prac, w szczególności informacji dotyczących funkcjonowania systemów służących do przetwarzania danych osobowych, do których zostałam(-łem) upoważniona(-ny) oraz haseł i zasad dostępu do tych systemów także po ustaniu umowy wiążącej mnie z Urzędem. Z chwilą ustania umowy zobowiązuję się do niezwłocznego zwrócenia wszelkich dokumentów oraz innych materiałów dotyczących danych osobowych.

6. Przyjmuję do wiadomości, że przetwarzanie danych osobowych z naruszeniem udzielonego upoważnienia może skutkować poniesieniem odpowiedzialności karnej.

---

Data i podpis Upoważnionego

Postępowanie dotyczące sporządzania rejestru czynności przetwarzania danych oraz rejestru kategorii czynności przetwarzania danych

CEL PROCEDURY Zapewnienie, przez administratora, zgodności z RODO (art. 5 ust. 2 RODO), czyli ze wskazanymi w tym akcie prawnym zasadami i warunkami przetwarzania danych osobowych.

#### ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

Kierownicy komórek organizacyjnych – w zakresie aktualności i poprawności informacji zawartych w rejestrach cząstkowych w ramach realizowanych procesów przetwarzania danych osobowych w zarządzanej komórce organizacyjnej.

KAG – w zakresie koordynowania oraz prowadzenia nadzoru nad prowadzeniem rejestru czynności przetwarzania dla Urzędu.

#### POSTANOWIENIA OGÓLNE PROCEDURY

1. Za sporządzenie rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania danych dla całego Urzędu odpowiada KAG.

3. Pierwsze rejestry czynności przetwarzania i rejestry kategorii czynności przetwarzania danych cząstkowe sporządzane zostaną na podstawie przeprowadzonej inwentaryzacji czynności przetwarzania danych. KAG przekaze do komórek organizacyjnych projekty rejestrów, o których mowa w ust. 1, zgodnie z właściwością celem ponownego uzgodnienia zapisów oraz ewentualnego uaktualnienia.

4. KAG nie rzadziej niż dwa razy w roku będzie występował do komórek organizacyjnych celem zapewnienia, że nie zmieniły się procesy przetwarzania oraz kategorie przetwarzanych danych w przypadku, poprzez przekazanie rejestrów, o których mowa w ust. 1, zgodnie z właściwością celem ponownego uzgodnienia zapisów oraz ewentualnego uaktualnienia.

5. Kierownicy komórek organizacyjnych Urzędu mają obowiązek na bieżąco informować KAG o wszelkich zmianach w procesach przetwarzania danych osobowych realizowanych w swoich komórkach, w szczególności dotyczących:

- 1) celów przetwarzania danych;
- 2) kategorii osób, których dane są przetwarzane;
- 3) zakresu przetwarzania danych;
- 4) podmiotów przetwarzających, którym dane są powierzane;
- 5) odbiorców danych, którym dane są udostępnione.



Postępowanie w zakresie zawierania umów lub porozumień w sprawie powierzenia przetwarzania danych osobowych

CEL PROCEDURY Zapewnienie zgodności z RODO (art. 5 ust. 2 RODO), czyli ze wskazanymi w tym akcie prawnym zasadami i warunkami przetwarzania danych osobowych.

ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY jest KAG

POSTANOWIENIA SZCZEGÓŁOWE PROCEDURY

Powierzenie przetwarzania danych przez Urząd

1.KAG zobowiązany jest informować IOD z tygodniowym wyprzedzeniem o zamiarze powierzenia przetwarzania danych osobowych i przekazać mu niezbędne informacje w tym zakresie, tj. szczegółowy opis na czym ma polegać przetwarzanie danych osobowych przez podmiot przetwarzający w celu uzgodnienia z IOD kryteriów wyboru podmiotu przetwarzającego.

2.Konsultacje z IOD, o których mowa w ust. 1, muszą odbyć się w szczególności przed złożeniem wniosku o wszczęcie postępowania na podstawie ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz.U. 2018 r. poz. 1986), a jeżeli nie jest wymagane stosowanie ustawy – przed inną procedurą wyboru kontrahenta.

3.Każda umowa, porozumienie lub aneks w sprawie powierzenia przetwarzania danych osobowych musi być zaparafowany przez IOD.

4.Informacje w zakresie umów lub porozumień (data zawarcia, podmiot) w sprawie przetwarzania danych osobowych muszą zostać zawarte w rejestrze czynności prowadzonym w Urzędzie.

5.Umowa w zakresie powierzenia przetwarzania danych osobowych powinna w szczególności zawierać:

1)cel przetwarzania danych;

2)oświadczenie procesora o zapewnieniu wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie powierzonych danych osobowych spełniało wymogi prawem przewidziane i chroniło prawa osób, których dane dotyczą;

3)rodzaj i zakres przekazanych danych;

4)informacje o zasadach dotyczących przeprowadzania kontroli w podmiotach przetwarzających dane osobowe w imieniu administratora ;

5)informacje o sposobie upoważniania osób, które w imieniu procesora będą przetwarzały dane osobowe;

- 6)informacje o sposobach zgłaszania naruszeń z zakresu ochrony danych osobowych;
- 7)informacje o sposobach postępowania z danymi osobowymi po zakończeniu realizacji umowy.

Urząd jako podmiot przetwarzający

1.Każda umowa lub porozumienie lub aneks w sprawie powierzenia przetwarzania danych osobowych musi być zaparafowany przez IOD.

2.Kategorie czynności, które zostały administratorowi powierzone do przetwarzania, muszą zostać zawarte w rejestrze kategorii czynności prowadzonym w Urzędzie.

**Wzór klauzuli informacyjnej w przypadku zbierania danych od osoby,  
której dane dotyczą**

Zgodnie z art. 13 ust. 1 i 2 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 informuję:

1. Administratorem Pani/ Pana<sup>1</sup> danych osobowych jest Burmistrz Prudnika, 48-200 Prudnik, Kościuszki 3, 48-200 Prudnik.

2. Z administratorem danych można się skontaktować poprzez adres mailowy um@prudnik.pl, lub pisemnie na adres siedziby administratora.

3. Z Inspektorem Ochrony Danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych w szczególności w zakresie korzystania z praw związanych z ich przetwarzaniem poprzez adres mailowy iodo@prudnik.pl lub pisemnie na adres siedziby administratora.

4. Podstawą prawną przetwarzania Pani/Pana<sup>1</sup> danych jest<sup>1</sup>:

1) art. 6 ust 1 lit. b RODO, tj. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

2) art. 6 ust. 1 lit. c RODO, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze w związku z .....

3) art. 6 ust. 1 lit. e RODO, tj. przetwarzanie jest niezbędne do wykonania zdania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Burmistrzowi w związku z .....

4) art. 6 ust. 1 lit. f RODO, tj. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Burmistrza w związku z prowadzonym .....

5. Pani/Pana<sup>1</sup> dane przetwarzane są w celu .....

6. Pani/Pana<sup>1</sup> dane osobowe będą udostępnione ..... w związku z .....

7. Pani/Pana<sup>1</sup> dane będą przechowywane przez okres wynikający z Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.

8. Przysługuje Pani/Panu<sup>1</sup> prawo do dostępu do swoich danych osobowych, prawo żądania ich sprostowania oraz ograniczenia ich przetwarzania.

9. Przysługuje Pani/ Panu<sup>1</sup> prawo do żądania usunięcia danych osobowych, jeżeli dane osobowe nie są niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane.

10. W zakresie udostępnienia danych przysługuje Pani/ Panu<sup>1</sup> prawo do wniesienia sprzeciwu wobec przetwarzania

11. Przysługuje Pani/ Panu<sup>1</sup> prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych w państwie członkowskim zwykłego pobytu, miejsca pracy lub miejsca popełnienia domniemanego naruszenia.

12. Pani/ Pana<sup>1</sup> dane nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

13. Podanie danych osobowych jest niezbędne i wynika z wyżej wskazanych przepisów prawa.

<sup>1</sup>niepotrzebne usunąć.

Wzór klauzuli informacyjnej w przypadku zbierania danych w sposób inny niż od osoby,  
której dane dotyczą

Zgodnie z art. 14 ust. 1 i 2 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 informuję, że:

1. Administratorem Pani/Pana<sup>1</sup> danych osobowych jest Burmistrz Prudnika, 48-200 Prudnik ul. Kościuszki 3.

2. Z administratorem danych można się skontaktować poprzez adres mailowy [um@prudnik.pl](mailto:um@prudnik.pl) lub pisemnie na adres siedziby administratora.

3. Z Inspektorem Ochrony Danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych, w szczególności w zakresie korzystania z praw związanych z ich przetwarzaniem poprzez adres mailowy [iodo@prudnik.pl](mailto:iodo@prudnik.pl) lub pisemnie na adres siedziby administratora.

4. Podstawą prawną przetwarzania Pani/Pana<sup>1</sup> danych jest<sup>1</sup>:

1) art. 6 ust. 1 lit. b RODO, tj. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

2) art. 6 ust. 1 lit. c RODO, tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze w związku z.....  
.....

3) art. 6 ust. 1 lit. e RODO, tj. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Burmistrzowi w związku z .....

4) art. 6 ust. 1 lit. f RODO, tj. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Ministra w związku z prowadzonym .....

5. Pani/Pana<sup>1</sup> dane zostały przekazane przez.....  
.....

6. Przetwarzanie danych osobowych obejmuje następujące kategorie Pani/Pana<sup>1</sup> danych:  
.....

7. Pani/Pana<sup>1</sup> dane osobowe będą udostępniane.....  
.....

8. Pani/Pana<sup>1</sup> dane będą przechowywane przez okres wynikający z Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych.

9. Przysługuje Pani/Pana<sup>1</sup> prawo do dostępu do swoich danych osobowych, prawo żądania ich sprostowania oraz ograniczenia ich przetwarzania.

10. Przysługuje Pani/Panu<sup>1</sup> prawo do żądania usunięcia danych osobowych, jeżeli dane osobowe nie są niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane.

11. W zakresie udostępnienia danych przysługuje Pani/Panu<sup>1</sup> prawo do wniesienia sprzeciwu wobec przetwarzania<sup>1</sup>.

12. Przysługuje Pani/Panu<sup>1</sup> również prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych w państwie członkowskim Pani/Pana<sup>1</sup> zwykłego pobytu, miejsca pracy lub miejsca popełnienia domniemanego naruszenia.

<sup>1</sup> Niepotrzebne usunąć.

### **Postępowanie dotyczące wniosku obywatela w zakresie przysługujących mu praw**

CEL PROCEDURY Sprecyzowanie i wdrożenie w Urzędzie jednolitej i przejrzystej procedury postępowania w przypadku złożenia przez obywatela wniosku w zakresie przysługujących mu praw.

#### **ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY**

1. Kierownicy komórek organizacyjnych Urzędu – w zakresie przyjmowania, realizacji i ewidencjonowania wniosku obywatela;
2. IOD – w zakresie koordynowania rozpatrywania wniosków obywateli.

#### **POSTANOWIENIA OGÓLNE PROCEDURY**

1. Korespondencję pisemną lub przesłaną za pośrednictwem e-PUAP, której treść wskazuje na wniosek obywatela w zakresie praw związanych z ochroną danych osobowych, przekazywana jest właściwemu kierownikowi komórki organizacyjnej.
2. W przypadku braku wystarczających informacji umożliwiających zidentyfikowanie komórki merytorycznej, do której powinien być przekazany wniosek, wniosek przekazuje się IOD, który ustala komórkę właściwą za jego realizację.
3. IOD przekazuje korespondencję do właściwej komórki, która jest zobowiązana do zrealizowania wniosku. W przypadku braku możliwości jego realizacji informację o przyczynach braku realizacji komórka merytoryczna właściwa do obsługi wniosku przesyła obywatelowi oraz IOD.
4. W przypadku gdy korespondencja, której treść wskazuje na wniosek obywatela w zakresie przysługujących mu praw związanych z ochroną danych osobowych, została przesłana bezpośrednio do komórki organizacyjnej Urzędu, komórka ta jest zobowiązana do niezwłocznego przekazania informacji o wniosku do IOD.
5. Komórka właściwa w sprawie rozpatrzenia wniosku, o którym mowa w ust. 1, informuje osobę, której wniosek dotyczy, oraz IOD o sposobie załatwienia wniosku.
9. Skargi i wnioski realizowane na podstawie Kodeksu postępowania administracyjnego obsługiwane są zgodnie z odrębną procedurą obowiązującą w Urzędzie. W przypadku pierwszego kontaktu z Urzędem do każdej korespondencji dołącza się stosowną klauzulę informacyjną.

## Rozdział I Prawa obywateli, których dane są przetwarzane w Urzędzie, wymagające wniosku

1. Obywatel, którego dane dotyczą, jest uprawniony do uzyskania potwierdzenia, czy w Urzędzie przetwarzane są jego dane osobowe. Jeżeli ma to miejsce, jest uprawniony do uzyskania dostępu do nich oraz pozyskania następujących informacji:

- 1) w jakim celu są przetwarzane jego dane osobowe;
- 2) jakich kategorii danych osobowych dotyczy przetwarzanie;
- 3) o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
- 4) o planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu;
- 5) o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
- 6) o prawie wniesienia skargi do organu nadzorczego;
- 7) o źródle danych, jeżeli nie zostały zebrane od osoby, której dotyczą.

2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, obywatel, którego dane dotyczą, ma prawo zostać poinformowany o odpowiednich zabezpieczeniach związanych z przekazaniem.

3. Jeżeli obywatel, którego dane dotyczą, zwróci się z wnioskiem o dostarczenie kopii jego danych osobowych podlegających przetwarzaniu, żądanie takie realizuje się bezpłatnie. Za wszelkie kolejne kopie, o które zwróci się ten obywatel, można pobrać opłatę. Opłata powinna obejmować jedynie faktyczne koszty sporządzenia kopii, tj. koszt papieru, koszty kserowania.

4. Jeżeli obywatel, którego dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się drogą elektroniczną po jednoznacznej weryfikacji tożsamości osoby, np. podaniu daty urodzenia, podaniu innej informacji, która była podana we wcześniejszej korespondencji, a co do której można mieć pewność, że będzie ją posiadać jedynie obywatel, którego dane dotyczą.

5. Kopię danych, o której mowa w ust. 3, wydaje się w postaci wydruku po ich przepisaniu lub skopiowaniu do ustrukturyzowanego powszechnie używanego formatu nadającego się do odczytu maszynowego. Nie wydaje się skanów dokumentów ani ich kserokopii, gdyż mogą zawierać dodatkowe dane nie dotyczące osoby występującej z wnioskiem.

6. Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.



## **Rozdział II Prawo do sprostowania danych**

1. Obywatel, którego dane dotyczą, ma prawo żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.

2. Ponadto obywatel, którego dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

3. Wniosek o sprostowanie lub uzupełnienie danych przekazywany jest w formie pisemnej lub drogą elektroniczną na adres Urzędu. Pracownik, który w ramach wykonywanych zadań przetwarza dane osoby wnioskującej, obowiązany jest dokonać weryfikacji przetwarzanych danych. Uzupełnienie danych następuje z uwzględnieniem celów przetwarzania.

4. Prawo do sprostowania danych nie znajduje zastosowania do danych osobowych, w odniesieniu do których tryb ich sprostowania lub uzupełnienia określają odrębne przepisy, np. procedura sprostowania błędów i omyłek zawartych w decyzji administracyjnej w trybie art. 113 Kodeksu postępowania administracyjnego

## **Rozdział III Prawo do żądania usunięcia danych**

1. Obywatel, którego dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących go danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

2) obywatel, którego dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;

3) dane osobowe były przetwarzane niezgodnie z prawem;

4) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie państwa członkowskiego, któremu podlega administrator.

2. Jeżeli dane osobowe zostały upublicznione, a na mocy ust. 1 istnieje obowiązek usunięcia tych danych osobowych, to (biorąc pod uwagę dostępną technologię i koszt realizacji) podejmuje się niezbędne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, że obywatel, którego dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

3. Przepisy ust. 1 i 2 nie mają zastosowania w zakresie, w jakim przetwarzanie jest niezbędne:

1) do korzystania z prawa do wolności wypowiedzi i informacji lub

2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii Europejskiej lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, lub

3) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania, lub

4) do ustalenia, dochodzenia lub obrony roszczeń.

#### **Rozdział IV Prawo do żądania ograniczenia przetwarzania**

1. Obywatel, którego dane dotyczą, ma prawo żądania ograniczenia przetwarzania jego danych osobowych.

2. Ograniczenie przetwarzania oznacza, że dane osobowe można jedynie przechowywać. Inne formy przetwarzania mogą mieć miejsce wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

3. Do ograniczenia może dojść w następujących przypadkach:

1) obywatel, którego dane dotyczą, kwestionuje prawidłowość danych osobowych; w tym przypadku ogranicza się przetwarzanie na okres pozwalający sprawdzić prawidłowość danych;

2) przetwarzanie jest niezgodne z prawem, a obywatel, którego dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

3) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

4) obywatel, którego dane dotyczą, wobec przetwarzania wniosła sprzeciw. W tym przypadku ogranicza się przetwarzanie do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu.

4. Ograniczenia przetwarzania dokonuje się poprzez odpowiednie oznaczenie danych osobowych, których dotyczy żądanie, przetwarzanych zarówno w formie tradycyjnej, jak i elektronicznej, tak aby każdy obywatel, który jest upoważniony do przetwarzania tych danych był świadomy że dane te można jedynie przechowywać.

5. Przed uchycieniem ograniczenia przetwarzania informuje się o tym osobę, która żądała ograniczenia.

#### **Rozdział V Prawo do przeniesienia danych**

1. Jeżeli przetwarzanie odbywa się na podstawie umowy, której stroną jest obywatel, którego dane dotyczą, oraz w sposób zautomatyzowany, obywatel ten ma prawo otrzymać w

ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe go dotyczące. Dotyczy to danych, które obywatel składający żądanie wcześniej dostarczył.

2. Wykonując prawo do przenoszenia danych na mocy ust. 1, obywatel, którego dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Urząd bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe i obywatel wykaże, że administrator, któremu mają zostać dane przekazane akceptuje taki sposób pozyskania danych.

3. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.

4. Wykonanie prawa, o którym mowa w ust. 1, pozostaje bez uszczerbku dla prawa do usunięcia danych.

5. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

## **Rozdział VI Prawo do wniesienia sprzeciwu wobec przetwarzania danych**

1. Jeżeli przetwarzanie oparte jest na przesłance wykonania zadania realizowanego w interesie publicznym, jakim jest między innymi dostęp do informacji publicznej, w tym umieszczanie danych w Biuletynie Informacji Publicznej, obywatel, którego dane dotyczą z przyczyn związanych z jego szczególną sytuacją, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących go danych osobowych.

2. Administratorowi nie wolno już przetwarzać danych osobowych, względem których wniesiono sprzeciw, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

3. W momencie złożenia sprzeciwu wobec przetwarzania administrator niezwłocznie ogranicza przetwarzanie i weryfikuje czy istnieją ważniejsze uzasadnione podstawy do przetwarzania niż interes osoby wnioskującej. Jeżeli administrator posiada podstawę prawną, o której mowa powyżej, informuje osobę wnioskującą o odmowie realizacji prawa wraz z uzasadnieniem decyzji. W przypadku gdy uzasadniona jest przesłanka do zrealizowania żądania postępuje się zgodnie z ust 2.

Wzór

Zgoda na przetwarzanie danych osobowych

Wyrażam zgodę na przetwarzanie przez Burmistrza Prudnika, 48-200 Prudnik, ul. Kościuszki 3 moich danych osobowych zawartych w ...../ w zakresie ..... w celu .....

Jestem świadoma(-my) przysługującego mi prawa do wycofania zgody, jak również faktu, że wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Zgodę mogę odwołać poprzez wysłanie maila opatrzonego podpisem kwalifikowanym na adres [iodo@prudnik.pl](mailto:iodo@prudnik.pl) lub za pośrednictwem potwierdzonego profilu e-PUAP z informacją o jej odwołaniu, w treści maila wskażę swoje imię i nazwisko, a w tytule wiadomości wpiszę „.....\*” lub listownie na adres Urzędu.

Podpis osoby wyrażającej zgodę

\* W tym miejscu należy podać nazwę czynności, w ramach której udzielono zgody, np. udział w konferencji/ szkoleniu

## Postępowanie w przypadku naruszenia ochrony danych osobowych

CEL PROCEDURY Sprecyzowanie i wdrożenie w Urzędzie jednolitej i przejrzystej procedury postępowania w przypadku naruszenia ochrony danych osobowych.

### ODPOWIEDZIALNI ZA WYKONANIE PROCEDURY

1.IOD w zakresie:

1)oceny czy zgłoszenie stanowi naruszenie ochrony danych osobowych:

a)jeżeli tak – czy może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych i w związku z tym wymaga zgłoszenia organowi nadzorcemu,

b)czy zidentyfikowane naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, co wiąże się z obowiązkiem zawiadomienia osób, których dane dotyczą;

2)dokumentowania spraw z zakresu naruszeń.

2. KAG w zakresie :

1)ewentualne zgłaszanie naruszeń w imieniu administratora do UODO;

2)ewentualne informowanie osób, których dane dotyczą o wystąpieniu naruszenia,

3.Administrator systemu informatycznego (ASI) – w sytuacji gdy naruszenie dotyczy systemów informatycznych, współdziała z IOD.

4.Pracownicy – w zakresie zgłaszania podejrzenia naruszenia lub naruszenia danych osobowych.

### POSTANOWIENIA OGÓLNE PROCEDURY

Procedura dotycząca postępowania w przypadku naruszeń ochrony danych osobowych realizowana jest w dwóch etapach:

1)wewnętrznym, którego celem jest ustalenie, czy zgłoszone zdarzenie jest naruszeniem oraz w jaki sposób zidentyfikowane zdarzenie wpłynie na ryzyko dla praw i wolności osób fizycznych;

2)zewnątrznym, którego celem jest zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego oraz poinformowanie osoby, której dane dotyczą, w przypadku gdy istnieje wysokie ryzyko dla praw i wolności osób fizycznych.

### POSTANOWIENIA SZCZEGÓŁOWE PROCEDURY

#### ROZDZIAŁ I – ETAP WEWNĘTRZNY

1.Każdy pracownik, stażysta, wolontariusz, praktykant oraz osoba realizująca zadania na podstawie umowy cywilnoprawnej, którzy stwierdzili lub podejrzewają wystąpienie zdarzenia, które stanowi naruszenie ochrony danych osobowych, ma obowiązek zgłoszenia tego faktu na

piśmie bezpośredniemu przełożonemu oraz na adres [iod@prudnik.pl](mailto:iod@prudnik.pl). W przypadku gdy zgłoszenie dotyczy systemów informatycznych stosowną informację należy przekazać również do Komórki organizacyjnej zajmującej się Informatyką, zgodnie z zasadami określonymi w Polityce Bezpieczeństwa Informacji.

2. Zgłoszenie zdarzenia mogącego być naruszeniem ochrony danych osobowych powinno zawierać:

- 1) opisanie symptomów naruszenia ochrony danych osobowych;
- 2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
- 3) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia;
- 4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzeń.

3. Stwierdzenie naruszenia następuje w momencie, kiedy IOD ma wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, prowadzące do naruszenia bezpieczeństwa danych osobowych.

4. Jeżeli naruszenie ochrony danych osobowych dotyczy systemu informatycznego, ASI w porozumieniu z IOD podejmuje niezbędne działania zabezpieczające niezwłocznie po otrzymaniu informacji, o której mowa w ust. 3. Szczegółowe zasady w tym zakresie opisuje Polityka Bezpieczeństwa Informacji.

5. Jeżeli naruszenie ochrony danych nie dotyczy systemu informatycznego i ma związek z naruszeniem zabezpieczeń fizycznych, odpowiednie czynności zabezpieczające podejmuje IOD, tj.:

- 1) nakazuje przerwanie pracy, zwłaszcza w zakresie przetwarzania danych osobowych, do czasu powiadomienia o zaistniałej sytuacji administratora;
- 2) działa w celu wyjaśnienia okoliczności zdarzenia;
- 3) przedstawia zalecenia w celu umożliwienia dalszego bezpiecznego przetwarzania danych.

6. Odmowa udzielenia wyjaśnień lub współpracy z IOD traktowana będzie jako naruszenie obowiązków pracowniczych.

7. Raport o naruszeniu danych osobowych opracowuje IOD według wzoru stanowiącego część niniejszej procedury. Raport przedstawiany jest Burmistrzowi.

## ROZDZIAŁ II – ETAP ZEWNĘTRZNY

1. W przypadku gdy naruszenie ochrony danych osobowych może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, musi być ono zgłoszone organowi nadzorcemu właściwemu zgodnie z art. 55 RODO bez zbędnej zwłoki, ale nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

2. W przypadku konieczności dokonania zgłoszenia naruszenia do organu nadzorczego pismo w tej sprawie przygotowuje pracownik KAG wyznaczony przez KAG. W zgłoszeniu takim należy w szczególności:

- 1) opisać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- 2) wskazać imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych;
- 3) opisać możliwe konsekwencje naruszenia ochrony danych osobowych;
- 4) opisać środki zastosowane lub proponowane w Urzędzie w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Jeżeli informacji, o których mowa w ust. 2, nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki w następujący sposób:

- 1) po dokonaniu pierwszego zgłoszenia można przekazywać na bieżąco organowi nadzorcemu aktualne informacje;
- 2) w przypadku uzyskania w toku dochodzenia dowodów na to, że opóźniono zdarzenie, a w rzeczywistości żadne naruszenie nie miało miejsca, informację tę można dodać do informacji już przekazanych do organu nadzorczego, a następnie zarejestrować zaistniałe zdarzenie jako niestanowiące naruszenia ochrony danych osobowych.

4. Do zgłoszenia przekazanego organowi nadzorcemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

5. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, bez zbędnej zwłoki zawiadamia się o tym osoby, których dane dotyczą.

6. Za realizację obowiązku wskazanego w ust. 5 odpowiada pracownik KAG wyznaczony przez KAG.

7. Zawiadomienie należy przygotować jasnym i prostym językiem.

8. Zawiadomienie, o którym mowa w ust. 5, nie jest wymagane, w następujących przypadkach:

- 1) w Urzędzie wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
- 2) w Urzędzie zastosowano następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;

3)wymagałoby ono niewspółmiernie dużego wysiłku: w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

9.Należy wykazać przed organem nadzorczym, że został spełniony przynajmniej jeden z warunków wskazanych w ust. 8 w przypadku braku powiadomienia osób, których dane naruszono.



**Raport o naruszeniu danych osobowych**

Sporządzający raport: Imię i nazwisko .....

Stanowisko (funkcja) .....<sup>1</sup>

Miejsce, dokładny czas i data naruszenia bezpieczeństwa informacji w tym ochrony danych osobowych (piętro, nr pokoju, godzina itp.):.....

.....

2)Osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia bezpieczeństwa informacji w tym ochrony danych osobowych):

.....

3)Charakter naruszenia (tj. nieuprawnione lub przypadkowe ujawnienie lub udostępnienie danych, wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania, brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną): .....

4)Informacje o danych, które zostały lub mogły zostać ujawnione:

.....

5)Zabezpieczone materiały lub inne dowody związane z wydarzeniem:.....

.....

6)Kategorie danych, których dotyczy naruszenie.....

.....

7)Kategorie osób, których dotyczy naruszenie.....

.....

8)Środki bezpieczeństwa zastosowane przed naruszeniem.....

.....

9)Krótki opis wydarzenia związanego z naruszeniem bezpieczeństwa informacji, w tym ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania): .....

Data: .....

Podpis: .....

