REGULAMIN OCHRONY DANYCH OSOBOWYCH W *MIEJSKIM PRZEDSIĘBIORSTWIE WODOCIĄGÓW I KANALIZACJI SP. Z O.O. W SIERADZU*

Właściciel dokumentu:

Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o. o. w Sieradzu

Sieradz, 25.05.2018 r.

Spis treści

I. Słownik pojęć

1. **Administrator Danych (Administrator)** - Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o. o. w Sieradzu, zwana dalej MPWiK Sp. z o.o., decydująca o celach i środkach przetwarzania danych osobowych, reprezentowana przez Zarząd.
2. **Inspektor Ochrony Danych Osobowych (IOD)** - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.
3. **Dane osobowe zwykłe, standardowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (tj. podmiot danych). Osobą możliwą do zidentyfikowania jest każda osoba fizyczna, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie Identyfikatora takiego jak: imię i nazwisko, numer identyfikacyjny (np. PESEL, NIP, nr dowodu osobistego), identyfikator internetowy jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej, inne – dane adresowe i teleadresowe, dane majątkowe.

4. **Dane osobowe szczególnej kategorii, (tzw. wrażliwe)** – dane osobowe ujawniające: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, dane dotyczące seksualności lub orientacji seksualnej osoby, dane dotyczące wyroków skazujących oraz naruszeń prawa.

5. **Przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, w tym: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

6. **Metody przetwarzania danych** – forma przetwarzania danych, tj. przetwarzanie danych w formie papierowej lub elektronicznej.

7. **Procesy przetwarzania danych** – przepływ danych w ramach wewnętrznych struktur organizacyjnych Administratora uwzględniający m.in. stanowiska pracy, na których dochodzi do przetwarzania danych oraz ewentualne przekazywanie danych do podmiotów zewnętrznych.

8. **Procedury przetwarzania danych** – dokumentacja regulująca zasady przetwarzania danych przez Administratora, w szczególności obowiązujące akty wewnętrzne (polityki, regulaminy) oraz faktycznie stosowane rozwiązania w toku przetwarzania danych

(tzw. zwyczaje pracownicze).

9. **Członek personelu** – osoba świadcząca pracę lub usługi na rzecz Administratora niezależnie od podstawy, formy i wymiaru zatrudnia (w szczególności na podstawie umowy o pracę, umowy cywilnoprawnej, umowy o pracę tymczasową, stałej współpracy gospodarczej).

II. Wprowadzenie

Administrator – MPWiK Sp. z o.o. – działając w oparciu o art. 24 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 (Dz.U.UE.L.2016.119.1), w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych, wprowadza niniejszym wewnętrzny system regulacji z zakresu danych osobowych. Opracowany on został na podstawie:

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (dalej RODO)
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 oraz z dnia 10 maja 2018 r. poz. 1000).

Celem niniejszego Regulaminu jest wdrożenie zasad - *privacy by design* oraz *privacy by default* w ramach systemu bezpieczeństwa danych. Administrator uwzględnienia ochronę danych na każdym etapie ich przetwarzania. Tym samym dla zapewnienia funkcjonalności rzeczonego systemu, Administrator wprowadza dokumentację systematyzującą procedury, procesy i zasady przetwarzania danych. Z uwagi na starania zapewnienia najwyższych standardów przetwarzania danych i zgodności z obowiązującym prawem, Administrator uświadamia wszystkich członków personelu o obowiązujących regulacjach i przyjętych procedurach minimalizując ryzyko nieuprawnionego, niezamierzonego przetwarzania danych przez członków personelu. Jednocześnie Regulamin nakłada na wszystkich członków personelu obowiązek weryfikacji przetwarzania danych w zgodzie z przyjętymi zasadami.

Administrator w celu zapewnienia bieżącej kontroli nad bezpieczeństwem przetwarzania danych powołał **Inspektora Ochrony Danych Osobowych** (dalej: IOD) iod@mpwiksieradz.pl

Przy powierzeniu funkcji IOD, Administrator kierował się umiejętnościami i kwalifikacjami kandydata, w tym w szczególności spełnieniem warunków określonych w art. 37 ust. 5 RODO, (kwalifikacje zawodowe, fachowa wiedzę na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia powierzonych zadań). Administrator odbiera oświadczenie o spełnieniu ww. warunków.

Administrator zawiadamia organ nadzoru o powołaniu IOD.

Dane kontaktowe Inspektora Ochrony Danych Osobowych udostępnione zostały każdemu członkowi personelu Administratora oraz osobom, których dane przetwarzane są przez Administratora poprzez: ujawnienie informacji w treści stosowanych klauzul umownych, informacyjnych, na stronie internetowej Administratora, poprzez wywieszenie w biurze Administratora.

III. Dane osobowe i ich przetwarzanie przez Administratora

Administrator w toku prac nad wewnętrznymi regulacjami z zakresu ochrony danych osobowych dokonał następujących czynności:

1. Zidentyfikował dane osobowe przetwarzane przez Administratora.
2. Zidentyfikował procesy, w ramach których przetwarzane są dane osobowe Administratora.
3. Dokonał analizy przetwarzania danych zgodnie z zasadami wynikającymi z RODO.
4. Dokonał ogólnej oceny ryzyka procesów przetwarzania.
5. Wdrożył przyjęte regulacje z ochrony danych osobowych w zgodności z zasadami i normami wynikającymi z RODO.

Dane osobowe przetwarzane przez Administratora obejmują zarówno dane osobowe zwykłe, jak i dane osobowe szczególnej kategorii – dane wrażliwe.

Poprzez dane osobowe rozumieć należy:

1. **Dane osobowe zwykłe, standardowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (tj. podmiot danych). Osobą możliwą do zidentyfikowania – podmiotem danych jest każda osoba fizyczna, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie Identyfikatora takiego jak:
   1) imię i nazwisko,
   2) numer identyfikacyjny (np. PESEL, NIP, nr dowodu osobistego),
   3) identyfikator internetowy
   4) jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

5) inne – dane adresowe i teleadresowe, dane majątkowe

2. **Dane osobowe wrażliwe, szczególnej kategorii** – rozumie się przez to dane ujawniające:
   1) pochodzenie rasowe lub etniczne,
   2) poglądy polityczne,
   3) przekonania religijne lub światopoglądowe,
   4) przynależność do związków zawodowych
   5) dane genetyczne lub dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej
   6) dane dotyczące zdrowia,
   7) dane dotyczące seksualności lub orientacji seksualnej osoby,
   8) dane dotyczące wyroków skazujących oraz naruszeń prawa

Administrator dokonał identyfikacji przetwarzanych danych w ramach występujących czynności przetwarzania danych.

IV. Zasady przetwarzania danych osobowych przez Administratora

Administrator w toku prac nad regulacjami z zakresu ochrony danych osobowych kierował się zasadami ujętymi w RODO, w tym:

1. Zasada zgodności z prawem, rzetelności i przejrzystości

Zgodnie z art. 5 ust. 1 lit. a RODO dane osobowe przetwarzane są zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

W myśl preambuły RODO powyższa zasada skutkuje koniecznością poinformowania osób fizycznych w sposób przejrzysty, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Jednocześnie zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach. Administrator powinien podać osobie, której dane dotyczą, wszelkie inne informacje niezbędne do zapewnienia rzetelności
i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych. Ponadto należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania. Jeżeli gromadzi się dane osobowe od osoby, której dane dotyczą, należy ją też poinformować, czy ma ona obowiązek je podać, oraz o konsekwencjach ich niepodania. Informacje te można przekazać w połączeniu ze standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób

przedstawią sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, powinny nadawać się do odczytu maszynowego.

2. Zasada ograniczenia celu przetwarzania danych

Zgodnie z art. 5 ust. 1 lit. b RODO dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Jednocześnie przetwarzanie danych osobowych do celów innych niż cele, w których dane te zostały pierwotnie zebrane, powinno być dozwolone wyłącznie w przypadkach, gdy jest zgodne z celami, w których dane osobowe zostały pierwotnie zebrane. Jeżeli administrator planuje przetwarzać dane osobowe w celu innym niż cel, w których dane osobowe zostały zebrane, powinien on przed takim dalszym przetwarzaniem poinformować osobę, której dane dotyczą, o tym innym celu oraz dostarczyć jej innych niezbędnych informacji.

3. Zasada minimalizacji danych

Zgodnie z art. 5 ust. 1 lit. c RODO dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Powyższe wymaga w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu.

4. Zasada prawidłowości danych

Zgodnie z art. 5 ust. 1 lit. d RODO dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość"). Gwarancja realizacji zasady prawidłowości danych wymaga stosowania odpowiednich rozwiązań technicznych i organizacyjnych umożliwiających korektę nieprawidłowych lub nieaktualnych danych.

5. Zasada ograniczenia przechowania danych

Zgodnie z art. 5 ust. 1 lit. e RODO dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Powyższe wymaga m.in. zapewnienia ograniczenia okresu przechowywania danych do niezbędnego minimum oraz wdrożenie odpowiednich procedur wyznaczających terminy przechowania danych (okresy retencji) lub procedur określających terminy okresowych przeglądów danych.

6. Zasada integralności i poufności danych

Zgodnie z art. 5 ust. 1 lit. f RODO dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową

utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

7. Zasada rozliczalności

Zgodnie z art. 5 ust. 2 RODO Administrator jest odpowiedzialny za przestrzeganie przepisów dotyczących zasad przetwarzania danych i musi być w stanie wykazać ich stosowanie („rozliczalność").

8. Zasada legalności

Procesy przetwarzania danych wymagają legalności źródła i podstawy przetwarzanych danych, którymi mogą być, zgodnie z art. 6 RODO:

- zgoda osoby, której dane dotyczą w zakresie celu wskazanego w udzielonej zgodzie
- umowa, której stroną jest osoba, której dane dotyczą a przetwarzanie danych jest niezbędne do wykonania umowy,
- przetwarzanie na podstawie przepisów prawa w ramach realizacji obowiązku prawnego ciążącego na administratorze;

Powyżej wskazane przesłanki legalizacyjne, mają charakter autonomiczny i równoprawny, co oznacza, że do spełnienia przez administratora zasady legalności wystarczające jest zaistnienie jednej spośród nich. Jednakże w przypadku warunku zgody, przyjmuje się, że nie jest co do zasady dopuszczalne jej wykorzystywanie do legalizacji przetwarzania, które swoje źródło ma w np. realizacji obowiązku lub przepisie prawa. Innymi słowy, opieranie legalności przetwarzania w oparciu o udzielone zgody nie powinno dotyczyć przetwarzania danych mających inne podstawy. Jednocześnie oznaczenie przesłanki legalizacyjnej, na której administrator opiera przetwarzanie danych, ma charakter uprzedni w stosunku do procesu przetwarzania.

W celu zapewnienia powyższych praw zostaje udostępniony formularz kontaktowy zawarty w załączniku nr 1 do niniejszego Regulaminu.

V. Realizacja zasad przetwarzania danych przez Administratora

Administrator przed przystąpieniem do przetwarzania danych zapewnił, ażeby przetwarzanie danych następowało na następujących warunkach:

- przetwarzanie następuje wyłącznie przez osoby upoważnione.
- Administrator dokonał inwentaryzacji danych ustalając kategorie, zakres danych oraz cele, metody i procesy przetwarzania, oznaczył przy tym obszary, (pomieszczenia) w obrębie których dozwolone jest przetwarzanie danych.

Samowolne przetwarzanie przez członków personelu, danych nieewidencjonowanych przez Administratora lub przetwarzanie w obszarach do tego nie przeznaczonych jest niedopuszczalne.

- Podmiot danych, przed przystąpieniem do przetwarzania jego danych uzyskał informację zgodnie z wymogami RODO. W tym celu Administrator wprowadził obowiązek stosowania klauzul informacyjnych, o treści ustalonej w Polityce przetwarzania danych osobowych i na zasadach w niej przewidzianych oraz utworzył kanały komunikacji.

- Administrator przed przystąpieniem do przetwarzania danych dokonał kategoryzacji celów oraz przeprowadził analizę zasadności zakresu przetwarzanych danych dla realizacji celów jego przetwarzania. Jednocześnie Administrator przyjął zasady retencji danych oraz procedury nadzorcze i kontrolne w zakresie ich przestrzegania.

Samowolne przetwarzanie przez członków personelu, danych osobowych dla innych celów niż ustalone przez Administratora lub przez dłuższy czas jest niedopuszczalne.

- Administrator wprowadził odpowiednie środki ochrony danych, w tym środki organizacyjne, fizyczne i techniczne.

VI. Postanowienia końcowe

Niniejszy Regulamin stanowi dokument y Administratora, z którego treścią zapoznani zostają m.in. wszyscy członkowie personelu Administratora.

Regulamin jest udostępniany osobom wszystkim zainteresowanym,

W sprawach nieuregulowanych w niniejszym Regulaminie i dokumentacji wewnętrznej Administratora z zakresu bezpieczeństwa danych zastosowanie mają przepisy RODO oraz aktów prawa powszechnie obowiązującego.

Załącznik nr 1 – Formularz kontaktowy

I. Dane Administratora		
MPWiK Sp. z o.o. w Sieradzu	*98-200 Sieradz, , ul. Górka Kłocka 14*	*iod@mpwiksieradz.pl*

II. Dane zgłaszającego			
Imię	Nazwisko	Dane adresowe	Dane kontaktowe

Preferowana przez zgłaszającego forma kontaktu
(wskazać formę tradycyjną – listowną lub elektroniczną)

III. Żądanie Zgłaszającego

III.A Żądanie dostępu i informacji
(należy zaznaczyć właściwe)

Wnoszę o udzielenie informacji, czy Administrator przetwarza moje dane osobowe, a jeżeli tak proszę o wskazanie:

- Jakie dane przetwarzane są przez Administratora (kategoria danych)
- W jakim celu Administrator przetwarza dane osobowe
- Jaki jest czas przetwarzania danych przez Administratora
- Kategorii odbiorców danych osobowych, w tym udostępnieniu danych poza obszar UE oraz podstawach udostępnienia
- Jakie prawa przysługują osobie, której dane przetwarza Administrator
- Źródła pozyskania danych przez Administratora
- Czy przetwarzanie obejmuje profilowanie

Wnoszę o przesłanie kopii danych przetwarzanych przez Administratora za pośrednictwem poczty elektronicznej …….. / na adres ……..

UZASADNIENIE

……
……
……

II.B Żądanie sprostowania danych

W związku z przetwarzaniem moich danych przez Administratora niniejszym informuję, że przetwarzane dane są nieprawidłowe.

……
……
……
……
……..

(należy wskazać, na czym polega wadliwość danych oraz wskazanie prawidłowych danych)

W związku z powyższym, wnoszę o ich sprostowanie.

Na czas prowadzenia czynności wyjaśniających przez Administratora, wnoszę / nie wnoszę o ograniczenie przetwarzania danych w ww. zakresie.

II.C Żądanie przeniesienia danych

W związku z przetwarzaniem moich danych przez Administratora w sposób zautomatyzowany, niniejszym wnoszę o przekazane przez Administratora kopii danych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego za pośrednictwem poczty elektronicznej ……..…. / na adres ……..

W związku z przetwarzaniem moich danych przez Administratora w sposób zautomatyzowany, niniejszym wnoszę o przekazanie kopii danych podmiotowi ……
…… (oznaczenie podmiotu, w tym dane kontaktowe)

UZASADNIENIE

……
……
……
……
……

III.D Żądanie usunięcia lub ograniczenia przetwarzania danych
(należy zaznaczyć właściwe)

Wnoszę o ograniczenie przetwarzania danych:

Wszystkich danych
Danych w zakresie ……

UZASADNIENIE

……
……
……
……
……
……

Wnoszę o usunięcie danych:

Wszystkich danych
Danych w zakresie ……

UZASADNIENIE

……
……
……
……
……
……

III.E Sprzeciw Podmiotu danych

POUCZENIE
Podmiot danych ma prawo do wniesienia sprzeciwu dotyczącego przetwarzania danych jego dotyczycących, wyłącznie wówczas, gdy:

1) Administrator przetwarza dane w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
   lub
2) Administrator przetwarza dane w celu realizacji jego prawnie uzasadnionych interesów.

Jeżeli przetwarzanie następuje na innej niż ww. podstawie, prawo do wniesienia sprzeciwu nie przysługuje.

Wnoszę o ograniczenie przetwarzania danych:

Wszystkich danych
Danych w zakresie ……

UZASADNIENIE

……
……
……
……

Lista załączników
(Jeżeli zgłaszający składa załączniki)

1. ……
2. ……
3. ……

Pouczenie

1. Rubryki formularza niedotyczące zgłoszenia należy przekreślić. Jeżeli cała treść żądania nie została ujęta w dedykowanej rubryce, dalszą część żądania należy zawrzeć na osobnych kartach.
2. Administrator powołał IOD odpowiedzialnych za przetwarzanie danych osobowych.
3. Administrator informuje, że przesłanie kopii przetwarzanych danych poprzedzone jest czynnościami weryfikującymi zgłoszenie, w szczególności środkami zabezpieczającymi przed nieuprawnionym udostępnieniem danych.
   Pierwsze udostępnienie danych na żądanie Podmiotu danych jest bezpłatne.
4. Podmiot danych może wnieść skargę do organu nadzoru.