Informacje dla Klientów opracowane na podstawie

Polityki **O**chrony **D**anych **O**sobowych

w Miejskim Zakładzie Gospodarki Komunalnej
sp. z o.o. w Nowej Soli.

Wydanie II – obowiązujące od 08.04.2019 r.

Niniejsza Polityka Ochrony Danych Osobowych jest dokumentem określającym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań **Rozporządzenia** PE i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (Dz.U.UE.L.2016.119.1; zwanym dalej **RODO** lub **Rozporządzeniem**) oraz obowiązującym ustawodawstwem krajowym w zakresie dotyczącym ochrony danych osobowych.

Polityka Ochrony Danych Osobowych (dalej Polityka lub PODO) stanowi jeden ze środków organizacyjnych mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z Rozporządzeniem oraz obowiązującymi przepisami prawa.

Zarząd Spółki realizuje i udostępnia Politykę w celu uświadomienia całej organizacji potrzeby ochrony danych osobowych, niezależnie od przyjmowanej przez nie formy - elektronicznej czy papierowej.

Bezpieczeństwo informacji odnosi się do wszystkich procesów związanych z przetwarzaniem danych osobowych: od momentu pozyskania lub wytworzenia, poprzez wszelkie inne czynności w tym: przechowywanie, przetwarzanie, przesyłanie, prezentowanie, udostępnianie, archiwizowanie oraz niszczenie.

Zarząd MZGK Sp. z o.o. w Nowej Soli angażuje się w rozwój i wdrożenie systemu bezpieczeństwa danych osobowych posiadanych przez Spółkę. Zarząd deklaruje stałe doskonalenie niniejszej Polityki.

Na wielu etapach przetwarzania danych najsłabszym ogniwem może być człowiek, dlatego Zarząd deklaruje podejmowanie działań związanych z edukacją pracowników w zakresie zachowania najwyższego poziomu bezpieczeństwa danych osobowych przetwarzanych w Spółce przy **wsparciu i zaangażowaniu kadry kierowniczej**. **Każdy kierownik ma obowiązek kontrolowania przestrzegania zasad ochrony danych osobowych w podległej komórce organizacyjnej.**

DEFINICJE

Dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak:
– imię i nazwisko,
– numer identyfikacyjny,
– dane o lokalizacji,
– identyfikator internetowy,
– jeden bądź kilka szczególnych czynników określających: fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Przetwarzanie danych osobowych – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub nie

zautomatyzowany, taką jak 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.

Administrator Danych Osobowych (ADO) - organ, jednostka organizacyjna, podmiot lub osoba **decydująca** o celach i środkach przetwarzania danych osobowych. W imieniu MZGK sp. z o.o. w Nowej Soli jako ADO został wyznaczony **Prezes** Spółki. Podczas nieobecności Prezesa, zgodnie ze stosownym pełnomocnictwem obowiązki ADO pełni Prokurent.

Administrator Systemu Informatycznego (ASI) - osoba fizyczna lub prawna odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych **w systemach informatycznych**, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach. W Spółce funkcję tę pełni **Informatyk.**

Inspektor Ochrony Danych (IOD) - osoba monitorująca i nadzorująca przestrzeganie przepisów o ochronie danych osobowych. IOD ma za zadanie informowanie i doradzanie w sprawach dotyczących ochrony danych osobowych oraz współpracuje i pełni funkcję punktu kontaktowego dla organu nadzorczego. IOD jest wyznaczany przez Prezesa Spółki.

Incydent - jest to naruszenie bezpieczeństwa informacji, pojedyncze zdarzenie lub seria zdarzeń, które zagraża jej poufności, dostępności lub integralności.

Osoba upoważniona lub użytkownik systemu (użytkownik) - osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych (**ADO**) dopuszczona, w zakresie w nim wskazanym do przetwarzania danych osobowych w systemie informatycznym i papierowym danej komórki organizacyjnej.

Osoba trzecia - każda osoba nieupoważniona i przez to nieuprawniona do dostępu do zbiorów danych osobowych będących w posiadaniu ADO. Osobą trzecią jest również osoba posiadająca upoważnienie wydane przez ADO podejmująca czynności w zakresie przekraczającym ramy upoważnienia.

Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.

Prezes Urzędu Ochrony Danych Osobowych (PUODO) - organ właściwy w zakresie ochrony danych osobowych na terytorium Polski, utworzony ustawą z 10 maja 2018 roku o ochronie danych osobowych. Jest również krajowym organem nadzorczym w rozumieniu ogólnego rozporządzenia o ochronie danych (RODO).

Rozporządzenie (RODO) – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)

System informatyczny (system) - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Zgoda osoby, której dane dotyczą - 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.

Zbiór danych - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

REGULAMIN OCHRONY DANYCH OSOBOWYCH

1. W Spółce obowiązuje regulamin, który ma na celu zapewnienie osobom przetwarzającym dane osobowe wiedzy dotyczącej bezpiecznych zasad przetwarzania - **Regulamin Ochrony Danych Osobowych**.
2. Po zapoznaniu się z zasadami ochrony danych osobowych, osoby przetwarzające zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania w **Oświadczeniu o poufności**.

ZGODNOŚĆ Z PRAWEM

Administrator zapewnia, że:

- dane są legalnie przetwarzane (na podstawie art. 6, 9 Rozporządzenia);
- dane osobowe są adekwatne w stosunku do celów przetwarzania (minimalizacja danych) i nie są przetwarzane dalej w sposób niezgodny z tymi celami;
- dane osobowe są przetwarzane rzetelnie, w sposób przejrzysty przez określony konkretny czas;
- wobec osób, których dane osobowe przetwarza Administrator wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14 Rozporządzenia) wraz ze wskazaniem przysługujących im uprawnień (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu). Informacje na temat przetwarzania danych osobowych w Spółce znajdują się na stronie internetowej www.mzgkns.pl, na stronie e-usług oraz w siedzibie Spółki w działach obsługi klienta. Klauzule informacyjne są przekazywane klientom/pełnomocnikom wraz z odpowiedzią na wniosek. Wskazanie sposobu zapoznania się z klauzulami informacyjnymi znajduje się w stopce służbowych e-maili pracowników, w zapowiedzi automatycznej sekretarki – centrala telefoniczna, w stopkach wystawianych faktur dla klientów (nie dotyczy faktur wystawianych za odbiór wody i odprowadzanie ścieków);
- zapewniono odpowiednią ochronę danych. W przypadkach powierzenia przetwarzania danych zawarto pisemne umowy powierzenia przetwarzania danych osobowych z podmiotami przetwarzającymi (art. 28 Rozporządzenia).

UPOWAŻNIENIA

1. Administrator odpowiada za nadawanie upoważnień - **Upoważnienie do przetwarzania danych osobowych** - w zbiorach papierowych oraz w systemach informatycznych.

2. Inspektor Ochrony Danych prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych.

UMOWY POWIERZENIA

1. W przypadku konieczności przetwarzania danych przez odrębne podmioty Administrator danych powierza ich przetwarzanie, w drodze umowy zawartej na piśmie (umowa powierzenia) określając m.in. przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, obowiązki i prawa Administratora.
2. Administrator korzysta z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi Rozporządzenia i chroniło prawa osób, których dane dotyczą.
3. Podmiot przetwarzający nie może korzystać z usług innego podmiotu przetwarzającego bez uprzedniej zgody Administratora. Administrator może wyrazić sprzeciw wobec dalszego podpowierzenia danych osobowych.
4. W kwestiach nieuregulowanych w niniejszym rozdziale przepisy RODO stosuje się wprost.

WSPÓŁADMINISTROWANIE

1. Administrator Danych Osobowych zgodnie z art. 26 RODO w zakresie przetwarzanych przez siebie danych osobowych, dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi.
2. Współadministrowanie danymi może zachodzić wówczas, jeżeli Administrator Danych oraz co najmniej jeden inny podmiot wspólnie ustalają cele i sposoby przetwarzania danych osobowych.
3. W przypadku przyjęcia modelu współadministrowania danymi, Współadministratorzy danych w drodze wspólnych uzgodnień, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.
4. W kwestiach nieuregulowanych w niniejszym rozdziale przepisy RODO stosuje się wprost.

POSTĘPOWANIE Z INCYDENTAMI

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia przełożonego/ASI/IOD w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych. W każdym przypadku IOD zgłasza takie przypadki ADO.
2. Instrukcja postępowania z incydentami definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
3. Instrukcja postępowania z incydentami opisana została w **Regulaminie Ochrony Danych Osobowych**

SZKOLENIA

1. Każda osoba **przed dopuszczeniem do przetwarzania danych osobowych** zobowiązana jest odbyć szkolenie oraz zapoznać się z obowiązującą dokumentacją ochrony danych osobowych.
2. Materiały szkoleniowe dla uczestników szkolenia są udostępnione każdemu pracownikowi, który przetwarza dane osobowe.
3. Po pierwszym przeszkoleniu z zasad ochrony danych osobowych, pracownicy zobowiązani są do złożenia deklaracji ich stosowania oraz potwierdzenia znajomości tych zasad - podpisując **Oświadczenie o poufności** - załącznik nr 8.
4. Dbając o bezpieczeństwo przetwarzanych danych osobowych Spółka deklaruje, że będzie organizować szkolenia dla pracowników, które obejmować będą zagadnienia dotyczące zachowywania odpowiedniego poziomu bezpieczeństwa danych osobowych przetwarzanych w Spółce.

PROCEDURA PRZYWRACANIA DOSTĘPNOŚCI DANYCH OSOBOWYCH W PRZYPADKU WYSTĄPIENIA INCYDENTU FIZYCZNEGO LUB TECHNICZNEGO

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie wystąpienia incydentu fizycznego lub technicznego. W przypadku wystąpienia ww. sytuacji decyzję związaną z dalszym postępowaniem podejmuje ADO po uprzedniej konsultacji z ASI i IOD.

WYKAZ ZABEZPIECZEŃ

1. W Rozporządzeniu o ochronie danych osobowych podkreślono, że przetwarzanie danych osobowych powinno odbywać się w zakresie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji.
2. Administrator wdrożył odpowiednie środki, aby zapewnić odporność sieci lub systemu informatycznego na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych.
3. Administrator prowadzi **Wykaz zabezpieczeń**, które stosuje w celu ochrony danych osobowych.
4. W wykazie wskazano stosowane zabezpieczenia techniczne, informatyczne i organizacyjne.
5. Wykaz jest na bieżąco aktualizowany.

AUDYTY

Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. W tym celu będą przeprowadzane przynajmniej raz w roku audyty z obszaru ochrony danych osobowych.