Zarządzenie Nr 71/2020
Burmistrza Miasta i Gminy Oleszyce
z dnia 30 września 2020 r.

w sprawie zmiany zarządzenia nr 86/2018 Burmistrza Miasta i Gminy Oleszyce z dnia 24 października 2018 r. w sprawie wprowadzenia Polityki ochrony danych osobowych

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), publ. Dz. Urz. UE L Nr 119, s. 1, **zarządza się, co następuje:**

§ 1. Do Polityki ochrony danych osobowych wprowadzonej Zarządzeniem Nr 86/2018 z dnia 24 października 2018 r. wprowadza się następujące zmiany:

1. Po poz. 17 „Wykaz załączników" dodaje się:

„***18. Rejestrowanie czynności przetwarzania***

1. *Wszystkie czynności przetwarzania realizowane przez Administratora zamieszcza się w Rejestrze czynności przetwarzania danych, który w celu jego obowiązywania wprowadza się odrębnym aktem prawa wewnętrznie obowiązującego.*
2. *Wszystkie czynności przetwarzania powierzone Administratorowi przez innego Administratora zamieszcza w Rejestrze wszystkich kategorii czynności przetwarzania, który w celu jego obowiązywania wprowadza się odrębnym aktem prawa wewnętrznie obowiązującego.*
3. *Jednostka powinna przestrzegać wszelkich zasad przetwarzania powierzonych jej danych nałożonych na podstawie obowiązujących przepisów prawa, umów powierzenia, innych instrumentów prawnych oraz dokumentach ramowych określających zasady takiego przetwarzania.*
4. *W przypadku zmian w przepisach prawa lub nałożenia na Jednostkę przez naczelne lub centralne organy administracji państwowej obowiązku wykonania zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej, w związku z realizacją których występuje konieczność przetwarzania danych osobowych, pracownicy uzyskujący taką informację zobowiązani są do poinformowania kierownika Referatu, który we współpracy z Inspektorem Ochrony Danych, na podstawie przekazanych informacji dokonuje uzupełnia lub zmian w Rejestrze czynności przetwarzania danych.*
5. *W przypadku uzyskania informacji przez pracownika Jednostki o występowaniu tejże Jednostki jako Podmiotu przetwarzającego dane – na podstawie umowy powierzenia przetwarzania danych lub innego instrumentu prawnego – pracownik ten jest*

zobowiązany do poinformowania kierownika Referatu, który we współpracy z Inspektorem Ochrony Danych, na podstawie przekazanych informacji dokonuje uzupełnia lub zmian w Rejestrze wszystkich kategorii czynności przetwarzania

6. *Rejestry, o których mowa w ust. 1 i 2 przyjmują formę pisemną, w tym formę elektroniczną, która powinna być prowadzona w systemie informatycznym równolegle z formę pisemną.*
7. *Administrator jest zobowiązany do udostępnienia ww. rejestrów na żądanie organu nadzorczego. Rejestry nie stanowią dokumentów udostępnianych na podstawie Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t. j. Dz. U. z 2019 r., poz. 1429) – Wyrok Wojewódzkiego Sądu Administracyjnego w Łodzi, z dnia 12 lutego 2019 r., sygn. akt II SAB/Łd 181/18.*
8. *IOD we współpracy z Administratorem, przygotowuje i aktualizuje rejestry, o których mowa w ust. 1 i 2.*

Objaśnienie:

Rejestr czynności przetwarzania danych *prowadzony jest przez Jednostkę w przypadku, w którym Jednostka występuje jako Administrator danych osobowych.*

W Rejestrze tym zamieszcza się następujące informacje:

a) *imię i nazwisko lub nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela administratora oraz inspektora ochrony danych;*
b) *cele przetwarzania;*
c) *opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;*
d) *kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;*
e) *gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;*
f) *jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;*
g) *jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.*

Rejestr wszystkich kategorii czynności przetwarzania *prowadzony jest przez Jednostkę, w przypadku, w którym Jednostka występuje jako Podmiot przetwarzający dane osobowe.*

W Rejestrze tym zamieszcza się wszystkie następujące informacje:

a) *imię i nazwisko lub nazwa oraz dane kontaktowe Podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa Podmiot przetwarzający, a gdy ma to zastosowanie - przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;*
b) *kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;*

c) *gdy ma to zastosowanie - przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;*

d) *jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.*

19. Zasady anonimizacji danych osobowych

1. *Użytkownik, sporządzający protokoły z posiedzeń rady gminy, komisji, uchwały i inne dokumenty, które mają zostać umieszczone w Biuletynie Informacji Publicznej Jednostki jest zobowiązany do oceny przedmiotowych dokumentów pod względem dopuszczalności publikacji danych osobowych osób fizycznych niepełniących funkcji publicznych lub kierowniczych.*
2. *W sytuacji stwierdzenia obecności danych osobowych osób fizycznych w dokumencie, o którym mowa w ust. 1, Użytkownik zobowiązany jest do dokonania analizy legalności publikacji danych osobowych w przedmiotowym dokumencie oraz w razie konieczności do dokonania anonimizacji zawartych w dokumencie danych osobowych osób fizycznych (np. imion, nazwisk, adresu, nr PESEL, wieku, numeru telefonu, stanu zdrowia itp.),*
3. *W przypadku dokumentów udostępnianych przez Administratora na podstawie obowiązujących przepisów o dostępie do informacji publicznej należy zastosować następujące zasady anonimizacji danych:*
   1) *w przypadku udostępniania informacji o osobie fizycznej anonimizacji podlegają:*
      a) *imię i nazwisko, chyba że dane te są zawarte w umowach podlegających publikacji w BIP,*
      b) *PESEL oraz NIP,*
      c) *data i miejsce urodzenia,*
      d) *numer dokumentu, za pomocą którego można zidentyfikować osobę fizyczną (np. dowód, paszport, prawo jazdy, legitymacja, koncesja, itp.),*
      e) *adres zamieszkania, zameldowania lub pobytu,*
      f) *numer tel. lub faksu,*
      g) *adres e-mail,*
      h) *numer konta bankowego,*
      i) *numer działki i obręb,*
      j) *numer księgi wieczystej,*
      k) *informacje o zobowiązaniach finansowych (chyba że dane te podlegają publikacji w BIP),*
      l) *informacje o stanie zdrowia, sytuacji finansowej, społecznej, itp.,*
      m) *inne dane pozwalające zidentyfikować osobę fizyczną lub naruszyć jej prawa i wolności,*

2) *w przypadku udostępniania wyciągów z rachunków bankowych lub dokumentacji księgowej (w tym faktur) anonimizacji podlegają:*
   a) *imię i nazwisko (chyba że dane te są zawarte w umowach podlegających publikacji w BIP),*
   b) *PESEL oraz NIP,*
   c) *adres zamieszkania, zameldowania lub pobytu,*
   d) *numer konta bankowego,*
3) *Anonimizacji nie podlega jednak imię i nazwisko usługodawcy lub nazwa firmy realizującej usługę, informacja o wykonanej usłudze oraz kwota, za jaką usługa została wykonana.*
4) *w przypadku udostępniania kopii innych dokumentów Jednostki dodatkowo anonimizacji podlegają wszystkie informacje, które mogą bezpośrednio zidentyfikować osobę fizyczną lub inne osoby fizyczne biorące udział w realizacji spraw.*

1. *Zasady anonimizacji opisane w niniejszym rozdziale stanowią jedynie reguły ogólne anonimizacji i powinny być każdorazow indywidualnie weryfikowane kiedy dochodzi do udostępniania danych.*
2. *Anonimizacji nie podlegają w żadnym przypadku:*
   1) *nazwy organów, urzędów oraz instytucji publicznych,*
   2) *nazwy organizacji międzynarodowych,*
   3) *nazwy sądów,*
   4) *nazwy spółek Skarbu Państwa,*
   5) *dane osób reprezentujących Administratora,*
   6) *dane pracowników Administratora w zakresie realizacji zadań określonych w regulaminie Jednostki,*
   7) *dane członków zespołów, komisji rad i innych powołanych do realizacji zadań,*
   8) *nazwy dokumentów, np. uchwała, zarządzenie, umowa, porozumienie, aneks, a także elementy dokumentów, które nie naruszają praw i wolności osoby,*
   9) *imiona i nazwiska autorów cytowanych książek, komentarzy, artykułów naukowych, jeśli ich prace były wykorzystywane w treści dokumentów urzędowych podlegających udostępnieniu,*
   10) *oznaczenie czasu, tj. informacje o latach, miesiącach, dniach, godzinach, przedziałach czasowych, jak też daty wytworzenia dokumentów, z wyjątkiem daty urodzenia osoby fizycznej,*
   11) *dane, co do których wyrażona jest pisemna zgoda na ich ujawnienie w BIP (np. petycje).*

20. Procedura przeglądu danych osobowych publikowanych w Biuletynie Informacji Publicznej

1. *Administrator udostępnia publicznie dane osobowe w Biuletynie Informacji Publicznej*

zgodnie z zasadami określonymi w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej (t. j. Dz. U. z 2019 r. poz. 1429) i innych przepisach powszechnie obowiązującego prawa.

2. *Administrator z uwzględnieniem zasady ograniczenia przechowywania zapewnia, że przechowuje dane osobowe publikowane w Biuletynie Informacji Publicznej w formie umożliwiającej identyfikację podmiotu danych przez okres nie dłuższy, niż jest to niezbędne do celów, w których te dane osobowe są przetwarzane (okres retencji).*
3. *W przypadkach gdy okres retencji danych osobowych publikowanych w Biuletynie Informacji Publicznej nie wynika wyraźnie z przepisów prawa, Administrator ustala niniejsze okresy samodzielnie, uwzględniając ogólne zasady przetwarzania danych osobowych przewidziane w RODO. Wszystkie ustalone okresy retencji zostają uwzględnione w treści Rejestru czynności przetwarzania danych prowadzonego przez Administratora, zwanego dalej Rejestrem.*
4. *Dane osobowe mogą być ponadto przetwarzane dłużej niż wynosi okres retencji, w przypadku gdy są one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (na zasadach określonych w art. 89 ust. 1 RODO), pod warunkiem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności podmiotów danych.*
5. *Administrator cyklicznie, nie rzadziej niż raz w roku dokonuje przeglądu danych osobowych publikowanych w Biuletynie Informacji Publicznej. Poza okresowymi przeglądami Administrator przeprowadza również przeglądy tych danych jeśli zajdzie przynajmniej jedna z poniższych sytuacji:*
   1) *zmienione zostaną powszechnie obowiązujące przepisy prawa mające wpływ na okres retencji,*
   2) *organ nadzorczy lub organ kontrolujący wydadzą zalecenia dotyczące przeglądu danych,*
   3) *zostanie wydana uzasadniona decyzja Administratora (o której osoby zatrudnione w organizacji Administratora oraz z nią współpracujące zostaną poinformowane).*
6. *Wszelkie przeglądy danych osobowych publikowanych w Biuletynie Informacji Publicznej podlegają dokumentowaniu w postaci stosownego sprawozdania i są przechowywane w dokumentacji ochrony danych osobowych.*

21. Zasady dotyczące dokonywania transmisji i utrwalania obrad Rady Gminy

1. *Administrator dokonuje transmisji i utrwalania obrad rady gminy zgodnie z art. 20 ust. 1b ustawy o samorządzie gminnym (t. j. Dz. U. 2018, poz. 994 ze zm.) „Obrady rady gminy są transmitowane i utrwalane za pomocą urządzeń rejestrujących obraz i dźwięk. Nagrania obrad są udostępniane w Biuletynie Informacji Publicznej i na stronie internetowej gminy oraz w inny sposób zwyczajowo przyjęty".*
2. *Przed rozpoczęciem obrad, Przewodniczący Rady Gminy:*

a) *informuje radnych i innych uczestników, iż obrady są transmitowane na żywo oraz informuje o obowiązkach w zakresie nieujawniania, bez uzasadnionej potrzeby, danych osobowych osób niebędących funkcjonariuszami publicznymi, niepełniącymi funkcji publicznej, ani niezwiązanymi z tą funkcją,*
b) *realizuje obowiązek informacyjny wynikający z art. 13 ust. 1 i 2 RODO wywieszając stosowną klauzulę informacyjną na drzwiach wejściowych do Sali Obrad.*

3. *Administrator dokonuję teletransmisji sesji za pośrednictwem strony internetowej Urzędu Miasta i Gminy Oleszyce (YouTube), której serwer znajduje się w na terytorium Europejskiego Obszaru Gospodarczego. W przypadku umieszczenia nagrania na serwerze państwa trzeciego należy uwzględnić wymagania stawiane w tym zakresie przez art. 44-49 RODO.*
4. *Administrator dysponuje własną kopią nagrania obrad, które udostępniane są w BIP i na stronie internetowej Urzędu Miasta i Gminy Oleszyce.*
5. *W przypadku umieszczenia nagrania na serwerze zewnętrznym Administrator zawiera stosowną umowę powierzenia z jego właścicielem.*
6. *Administrator lub wyznaczona przez Administratora osoba przygotowując protokół, stenogram lub nagranie z takiego posiedzenia, w związku z jego udostępnieniem publicznym – zobowiązany jest do ochrony prawa do prywatności osób fizycznych, w tym ochrony ich danych osobowych. W związku z powyższym, jeżeli przy przygotowaniu ww. materiałów pojawią się dane osobowe osób niebędących funkcjonariuszami publicznymi, niepełniącymi funkcji publicznych, ani niezwiązanych z tymi funkcjami, dokonuje się anonimizacji takich danych.*
7. *Administrator lub wyznaczona przez Administratora okresowo dokonuje przeglądu nagrań z posiedzeń organów kolegialnych rady jednostki samorządu terytorialnego, pod kątem ewentualnych nieprawidłowości związanych z brakiem anonimizacji danych osobowych.*

22. *Zasady postępowania z dokumentami papierowymi zawierającymi dane osobowe*

1. *W stosunku do dokumentów papierowych stanowiących wydruki z systemu informatycznego Jednostki, Użytkowników obowiązują następujące środki ostrożności:*
   1) *wydruki z systemu informatycznego i wszelkie dokumenty zawierające dane osobowe powinny być niedostępne dla osób trzecich,*
   2) *wydruki z systemu informatycznego i wszelkie dokumenty zawierające dane osobowe nie mogą być pozostawione w drukarce lub kserokopiarce ogólnodostępnej,*
   3) *wydruki niepotrzebne i nieprzydatne powinny być na bieżąco niszczone za pomocą niszczarki,*
   4) *dokumenty zawierające dane osobowe, których nie można zniszczyć z przyczyn technicznych lub formalnych, powinny być składowane w miejscu z ograniczonym dostępem, systematycznie weryfikowane, a następnie archiwizowane zgodnie z obowiązującymi w tym zakresie przepisami..*

23. Zasady bezpiecznej pracy

1. Każdy Użytkownik zobowiązany jest do stosowania następujących zasad bezpieczeństwa:
   1) **polityki „czystego biurka"** - w trakcie pracy Użytkownik powinien mieć na biurku tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy materiały zawierające dane, wymagające szczególnej ochrony powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu dnia pracy każdy Użytkownik zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających istotne dane, w celu uniemożliwienia dostępu do nich osób nieupoważnionych,
   2) **polityki „czystego ekranu"** - w przypadku chwilowego opuszczenia stanowiska pracy Użytkownik zobowiązany jest do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane. Ponadto w trakcie pracy Użytkownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych,
   3) takiego ustawienia monitora, aby osoby niepowołane nie mogły zapoznać się z informacjami wyświetlanymi na monitorze. W przeciwnym wypadku należy wyposażyć monitor w odpowiedni filtr prywatyzujący,
   4) bieżącego niszczenia w niszczarce niepotrzebnej dokumentacji papierowej oraz przechowywania pozostałej dokumentacji papierowej w zabezpieczonych szafach, zamykanych przynajmniej na klucz,
   5) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej,
   6) zachowania w poufności wszelkich informacji w tym danych osobowych poprzez złożenie stosownego oświadczenia,
   7) niepozostawiania klucza w drzwiach biurowych po zewnętrznej stronie pomieszczenia,
   8) niepozostawiania pomieszczeń biurowych bez opieki.

24. Zarządzanie ciągłością działania

1. Zadania związane z zapewnieniem ciągłości działania opracowywane są w celu ograniczenia ryzyka wynikającego z codziennej pracy Jednostki, w tym w obszarze przetwarzania danych osobowych.
2. Plany ciągłości działania uwzględniają ryzyko w obszarze przetwarzania danych osobowych.
3. Administrator wyznacza osobę odpowiedzialną za uruchomienie planu ciągłości działania oraz prawidłowość przeprowadzanych testów planów ciągłości.
4. W szczególnych przypadkach Administrator, wspólnie z osobą odpowiedzialną za plan ciągłości działania, może opracować szczegółowy zestaw planów ciągłości działania, w

tym w obszarze przetwarzania danych osobowych.

25. Zarządzanie ryzykiem

1. *Administrator analizuje możliwe sytuacje i naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zwane dalej „analizami ryzyka".*
2. *Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii,*
3. *Analiza ryzyka powinna zapewniać:*
   1) *zidentyfikowanie ryzyka,*
   2) *oszacowanie ryzyka z punktu widzenia następstw dla działalności Jednostki oraz prawdopodobieństwa wystąpienia takiego ryzyka,*
   3) *informowanie o następstwach wystąpienia ryzyka,*
   4) *ustanowienie priorytetów w postępowaniu z ryzykiem,*
   5) *regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem,*
   6) *zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem.*
4. *Administrator dokumentuje wykonaną analizę ryzyka w postaci raportu.*
5. *Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w przypadkach, w których zgodnie z analizą ryzyka, ryzyko naruszenia praw i wolności osób jest wysokie oraz w każdym przypadku, gdy wymagają tego obowiązujące przepisy prawa i wytyczne Prezesa Urzędu Ochrony Danych Osobowych..*

26. Ochrona danych osobowych w fazie projektowania i domyślna ochrona danych osobowych

1. *Obowiązek uwzględnienia ochrony danych w fazie projektowania spoczywa na Administratorze. Ponadto w przypadku, gdy do przetwarzania wykorzystywane będą narzędzia dostarczane Administratorowi przez zewnętrznych dostawców wymagane jest zaangażowanie tego podmiotu. W przypadku dostawcy będącego podmiotem przetwarzającym uwzględnienia ochrony danych w fazie projektowania oparte jest na zasadach wynikających z art. 28 RODO.*
2. *Kluczowym wymogiem związanym z ochroną danych osobowych w fazie projektowania i domyślną ochrony danych jest niedopuszczenie do przetwarzania danych w sposób, który naruszałby poszczególne wymogi RODO poprzez:*
   1) *zebranie informacji o celach danego projektu oraz planowanych środkach realizacji tych celów,*
   2) *określenie adekwatnych - dla danego projektu - środków technicznych i organizacyjnych służących do ochrony danych osobowych,*

3) *ocenę czy z projektem łączą się ryzyka dla praw lub wolności i przyjęcia określonego mechanizmu postępowania z tym ryzykiem (ocena ryzyka może doprowadzić do konieczności przeprowadzenia pełnej oceny skutków a nawet uprzednich konsultacji z Prezesem Urzędu Ochrony Danych Osobowych),*
4) *przypisanie ról w organizacji w zakresie dokonywania ww ocen,*
5) *przeszkolenie pracowników aby przed rozpoczęciem przetwarzania (nowego projektu).*

3. *Wymóg ochrony danych osobowych w fazie projektowania wymaga nie tylko oceny danego procesu przetwarzania danych przed jego rozpoczęciem ale także monitorowania zgodności w czasie przetwarzania. Z punktu widzenia mechanizmu oceny nowych projektów i zarządzania projektami wprowadzono Rejestr czynności przetwarzania danych, który powinien podlegać bieżącym aktualizacjom."*

§ 2. Zarządzenie wchodzi w życie z dniem podpisania

BURMISTRZ
mgr inż. Andrzej Gryniewicz