Zarządzenie nr 34.2018
Wójta Gminy Młodzieszyn
z dnia 25 maja 2018 r.

w sprawie wprowadzenia zmian w obowiązujących w Urzędzie Gminy w Młodzieszynie Polityki Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych wprowadzonych Zarządzeniem nr 24.2018 Wójta Gminy Młodzieszyn z dnia 05.04.2018 r. oraz zmiany Zarządzenia nr 25.2018 Wójta Gminy Młodzieszyn z dnia 05.04.2018 r. w sprawie powierzenia obowiązków w zakresie ochrony danych osobowych

W związku z wejściem w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych) zarządzam co następuje:

§ 1

W obowiązujących w Urzędzie Gminy w Młodzieszynie Polityce Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych wprowadzam następujące zmiany:

1. Dotychczasowy § 1 ust. 2 Polityki Bezpieczeństwa Danych Osobowych otrzymuje brzmienie:
   „Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).
2. Dotychczasowy § 2 ust. 1 pkt. 1 Polityki Bezpieczeństwa Danych Osobowych otrzymuje brzmienie:
   „zbiorze danych – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie”
3. Dotychczasowy § 2 ust. 1 pkt. 2 Polityki Bezpieczeństwa Danych Osobowych otrzymuje brzmienie:
   „przetwarzaniu danych rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, 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”
4. Dotychczasowy § 2 ust. 1 pkt. 7 Polityki Bezpieczeństwa Danych Osobowych otrzymuje brzmienie:
   „Inspektorze Ochrony Danych Osobowych (dalej IODO lub Inspektor) rozumie się przez to osobę nadzorującą przestrzeganie zasad ochrony przetwarzanych danych osobowych i innych informacji prawem chronionych. Nadzoruje on stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez

osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem, lub zniszczeniem, a także przeprowadzi kontrole w zakresie określonym regulacjami wewnętrznymi Urzędu"

5. W § 2 ust. 1 Polityki Bezpieczeństwa Danych Osobowych po punkcie 11 dodaje się pkt. 12 i 13 w brzmieniu:
   „12. Podmiocie przetwarzającym rozumie się przez to organizację lub osobę, której Urząd powierzył przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna obsługa prawna).
   13. Profilowaniu rozumie się przez to dowolną formę 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."
6. Użyte w Polityce Bezpieczeństwa Danych Osobowych w różnych formach i przypadkach sformułowanie „koordynator ds. ochrony danych osobowych" zastępuje się w odpowiedniej formie i przypadku sformułowaniem „Inspektor Ochrony Danych Osobowych".
7. Dotychczasowy § 13 ust. 4 Polityki Bezpieczeństwa Danych Osobowych otrzymuje brzmienie:
   „Przetwarzanie danych zwykłych jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków:
   a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   b) 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;
   c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
   d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
   f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.
   Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.
8. W § 13 Polityki Bezpieczeństwa Danych Osobowych po ust. 4 dodaje się ust. 4a w brzmieniu:
   „Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby chyba, że spełniony jest jeden z poniższych warunków:
   a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;

b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

9. W § 13 Polityki Bezpieczeństwa Danych Osobowych skreśla się ust. 6.
10. W § 14 Polityki Bezpieczeństwa Danych Osobowych skreśla się pkt 3.
11. Dotychczasowy § 17 ust. 3 pkt 1 Polityki Bezpieczeństwa Danych Osobowych otrzymuje brzmienie:
    „pisemnego wnioskowania do Inspektora Ochrony Danych Osobowych o zarejestrowania nowych czynności przetwarzania danych"
12. Dotychczasowy § 18 Polityki Bezpieczeństwa Danych Osobowych otrzymuje brzmienie;

„1. Rejestr Czynności Przetwarzania Danych stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

2. Administrator prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

3. Rejestr jest jednym z podstawowych narzędzi umożliwiających Administratorowi rozliczanie obowiązków ochrony danych.

4. W Rejestrze, dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb Rejestru, Administrator odnotowuje co najmniej:

1) nazwę czynności,
2) cel przetwarzania,
3) opis kategorii osób,
4) opis kategorii danych,
5) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Administratora, jeśli podstawą jest uzasadniony interes,
6) sposób zbierania danych,
7) opis kategorii odbiorców danych (w tym przetwarzających),
8) informację o przekazaniu poza EU/EOG;
9) ogólny opis technicznych i organizacyjnych środków ochrony danych.

5. Wzór Rejestru stanowi Załącznik nr 2 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych". Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Urząd rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

6. Osoby odpowiedzialne za poszczególne czynności przetwarzania zobowiązane są do pisemnego zgłaszania Inspektorowi Ochrony Danych Osobowych konieczności aktualizacji zarejestrowanych czynności przetwarzania.

7. Informatyk odpowiedzialny jest za pisemne zgłaszanie do Inspektora Ochrony Danych Osobowych nazw programów wykorzystywanych do przetwarzania danych osobowych określonych w Załączniku nr 2 do Polityki."

13. Skreśla się § 19 Polityki Bezpieczeństwa Danych Osobowych.
14. Po § 27 Polityki Bezpieczeństwa Danych Osobowych dodaje się § 27a w brzmieniu:
„W przypadku naruszenia ochrony danych osobowych skutkującym ryzykiem naruszenia praw lub wolności osób fizycznych Administrator danych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia naruszenia do organu nadzorczego stanowi załącznik nr 3.
15. Po Rozdziale III Przetwarzanie danych osobowych Polityki Bezpieczeństwa Danych Osobowych dodaje się Rozdział IIIA Obowiązki informacyjne, zawiadomienia i realizacja praw osób, których dane dotyczą w brzmieniu:

„§ 19a

1. Przetwarzanie danych może opierać się jedynie w oparciu o podstawy wskazane w Polityce Bezpieczeństwa Danych Osobowych, na wyraźne polecenie Administratora i pod jego nadzorem.

2. Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

3. Przed przystąpieniem do zbierania danych lub zmianą celu przetwarzania wszyscy pracownicy, współpracownicy, partnerzy Administratora danych są zobowiązani do wypełniani obowiązku informacyjnego względem osób, których dane dotyczą. Wzór informacji w przypadku pozyskiwania danych osobowych od osoby, której dane dotyczą określa załącznik nr 4 do Polityki.
4. Jeżeli przetwarzanie danych odbywa się na podstawie zgody osoby, której dane dotyczą wszyscy pracownicy, współpracownicy, partnerzy Administratora danych są zobowiązani do uzyskania zgody przed przystąpieniem do przetwarzania danych. Wzór zgody określa załącznik nr 5 do Polityki.

§ 19b

1. Osoba, której dane dotyczą, w zależności od podstawy przetwarzania ma prawo do:
   1) Dostępu do danych
   2) Sprostowania i uzupełnienia danych
   3) „Bycia zapomnianym"
   4) Ograniczenia przetwarzania
   5) Przenoszenia danych
   6) Sprzeciwu
   7) Ludzkiej interwencji przy zautomatyzowanym przetwarzaniu.
2. Żądania osoby, której dane dotyczą mogą być składane osobiście lub przez pełnomocnika w formie:
   1) pisemnej – osobiście albo przesyłką pocztową w rozumieniu art. 3 pkt 21 ustawy
   2) z dnia 23 listopada 2012 r. - Prawo pocztowe (Dz.U. z 2017 r. poz. 1481);
   3) ustnie - telefonicznie albo osobiście do protokołu podczas wizyty osoby
   4) w Urzędzie;
   5) w formie elektronicznej z wykorzystaniem środków komunikacji elektronicznej, ile takie środki zostały do tego celu wskazane przez Urząd;
   6) bezpośrednio do IODO.
3. Na żądanie osoby, której dane dotyczą wszyscy pracownicy, współpracownicy, partnerzy Administratora danych są zobowiązani do potwierdzenia otrzymania żądania w uzgodniony z osobą sposób.
4. W przypadku złożenia żądania ustnie wszyscy pracownicy, współpracownicy, partnerzy Administratora danych są zobowiązani sporządzić notatkę służbową zawierającą co najmniej następujące dane:
   1) Dane zgłaszającego,
   2) Opis żądania,
   3) Datę otrzymania żądania,
   4) Datę sporządzenia notatki służbowej.
5. W przypadku złożenia żądania w formie pisemnej, pracownik upoważniony do odbioru korespondencji odnotowuje na żądaniu datę jego wniesienia.
6. Żądania przesłane drogą elektroniczną należy wydrukować.
7. W przypadku uzasadnionych wątpliwości co do tożsamości osoby składającej żądanie wszyscy pracownicy, współpracownicy, partnerzy Administratora danych mogą żądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.
8. Postępowanie w zakresie rozpatrzenia żądania rozpoczyna się od daty wpływu lub ustnego zgłoszenia żądania.
9. Wszelkie żądania pracownicy, współpracownicy, partnerzy Administratora danych są zobowiązani niezwłocznie przekazać Administratorowi danych lub IODO.

10. Administrator danych prowadzi rejestr żądań osób, których dane dotyczą. Wzór rejestru stanowi załącznik nr 6 do Polityki.
11. Administrator danych, po konsultacji z IODO, bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem lub o potrzebie przedłużenia terminu, nie dłużej jednak niż o kolejne dwa miesiące, z uwagi na skomplikowany charakter żądania lub liczbę żądań podając uzasadnienie opóźnienia.
12. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.
13. Jeżeli Administrator danych nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

§ 19c

1. Podmiot występujący o udostępnienie informacji, inny aniżeli osoba której dane dotyczą, powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne i czy nie będzie ono stanowić naruszenia zasad ochrony informacji.
2. Przetwarzanie, w tym udostępnianie informacji w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne jedynie w przypadkach określonych w obowiązujących przepisach o ochronie danych osobowych.

16. Po Rozdziale III Przetwarzanie danych osobowych Polityki Bezpieczeństwa Danych Osobowych dodaje się Rozdział IIIB Porozumienia i kontakty ze stronami zewnętrznymi w brzmieniu:

„§ 19d

1. W przypadku zawierania umów z firmami zewnętrznymi mającymi wpływ na funkcjonowanie kluczowych elementów systemu zarządzania bezpieczeństwem informacji należy zawrzeć umowy powierzenia i określić w nich następujące wymagania bezpieczeństwa:
   1) Zakres i cel czynności oraz danych mających być przedmiotem współpracy z firmą zewnętrzną.
   2) Zakresy odpowiedzialności w przypadku utraty lub ujawnienia danych.
   3) Własność informacji i oprogramowania oraz obowiązki w zakresie ochrony danych osobowych.
   4) Specjalne zabezpieczenia, które mogą być wymagane do ochrony informacji szczególnie chronionych, takich jak dane finansowe czy też identyfikatory i hasła dostępu.
   5) Warunki dostępu do informacji, zobowiązanie do zachowania w tajemnicy czynnika uwierzytelniającego.
   6) Definicje informacji, które mają być chronione (np. informacji poufnych).
   7) Spodziewany czas trwania umowy, łącznie z przypadkami, w których obowiązek zachowania poufności może być bezterminowy.
   8) Wymagane działania w momencie zakończenia umowy.
   9) Zasady zwrotu lub niszczenia informacji przy zakończeniu umowy.
   10) Działania podejmowane w przypadku naruszenia warunków umowy.
   11) Ustalenia dotyczące licencji, własności kodu i prawa do własności intelektualnej.
   12) Zasady testowania przed instalacją w celu wykrycia kodu złośliwego i koni trojańskich.

2. Inspektor Ochrony Danych Osobowych prowadzi wykaz podmiotów zewnętrznych. Wykaz stanowi załącznik nr 7 do Polityki.

17. Załącznik nr 2 do Polityki bezpieczeństwa danych osobowych otrzymuje brzmienie nadane Załącznikiem nr 1 do niniejszego Zarządzenia.
18. Załącznik nr 3 do Polityki bezpieczeństwa danych osobowych otrzymuje brzmienie nadane Załącznikiem nr 2 do niniejszego Zarządzenia.
19. Wprowadza się do Polityki bezpieczeństwa danych osobowych załącznik nr 4 w brzmieniu nadanym Załącznikiem nr 3 do niniejszego Zarządzenia.
20. Wprowadza się do Polityki bezpieczeństwa danych osobowych załącznik nr 5 w brzmieniu nadanym Załącznikiem nr 4 do niniejszego Zarządzenia.
21. Wprowadza się do Polityki bezpieczeństwa danych osobowych załącznik nr 6 w brzmieniu nadanym Załącznikiem nr 5 do niniejszego Zarządzenia.
22. Wprowadza się do Polityki bezpieczeństwa danych osobowych załącznik nr 7 w brzmieniu nadanym Załącznikiem nr 6 do niniejszego Zarządzenia.
23. Dotychczasowy § 1 ust. 2 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych otrzymuje brzmienie:
„2. Niniejsza Instrukcja została opracowana zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).
24. Dotychczasowy § 3 ust. 1 pkt. 1 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych otrzymuje brzmienie:
„zbiorze danych – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie"
25. Dotychczasowy § 3 ust. 1 pkt. 2 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych otrzymuje brzmienie:
„przetwarzaniu danych rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, 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"
26. Dotychczasowy § 3 ust. 1 pkt. 7 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych otrzymuje brzmienie:
„Inspektorze Ochrony Danych Osobowych (dalej IODO lub Inspektor) rozumie się przez to osobę nadzorującą przestrzeganie zasad ochrony przetwarzanych danych osobowych i innych informacji prawem chronionych. Nadzoruje on stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem, lub zniszczeniem, a także przeprowadzi kontrole w zakresie określonym regulacjami wewnętrznymi Urzędu"
27. W § 3 ust. 1 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych po punkcie 11 dodaje się pkt. 12 i 13 w brzmieniu:

„12. Podmiocie przetwarzającym rozumie się przez to organizację lub osobę, której Urząd powierzył przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna obsługa prawna).

13. Profilowaniu rozumie się przez to dowolną formę 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."

28. Użyte w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w różnych formach i przypadkach sformułowanie „koordynator ds. ochrony danych osobowych" zastępuje się w odpowiedniej formie i przypadku sformułowaniem „Inspektor Ochrony Danych Osobowych".
29. Dotychczasowy § 5 ust. 2 pkt. 1 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych otrzymuje brzmienie
„w systemie informatycznym nie są przetwarzane dane, o których mowa w art. 9 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych)".
30. Dotychczasowy § 5 ust. 3 pkt. 1 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych otrzymuje brzmienie:
„w systemie informatycznym są przetwarzane dane, o których mowa w art. 9 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych)".
31. Dotychczasowy § 32 ust. 2 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych otrzymuje brzmienie:
„W przypadku przekazywania urządzeń lub nośników zawierających dane osobowe, zwłaszcza dane, o których mowa w art. 9 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych), poza obszar przetwarzania danych osobowych, zabezpiecza się je w sposób zapewniający poufność i integralność tych danych, przez co rozumie się:
    1) Ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieuprawnionymi, lub
    2) Stosowanie metod kryptograficznych, lub
    3) Stosowanie odpowiednich zabezpieczeń fizycznych, lub
    4) W zależności od stopnia zagrożenia zalecane jest stosowanie kombinacji wyżej wymienionych zabezpieczeń".
32. Dotychczasowy § 57 ust. 1 pkt. 4 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych otrzymuje brzmienie:
„informacji o odbiorcach, o których mowa w art. 4 pkt 9 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych), którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia."
33. Dotychczasowy § 57 ust. 1 pkt. 5 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych otrzymuje brzmienie:

„sprzeciwu, o których mowa w art. 21 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych), którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia."

34. Załącznik nr 1 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych otrzymuje brzmienie nadane Załącznikiem nr 7 do niniejszego Zarządzenia.
35. Załącznik nr 5 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych otrzymuje brzmienie nadane Załącznikiem nr 8 do niniejszego Zarządzenia.

§ 2

W Zarządzeniu nr 25.2018 Wójta Gminy Młodzieszyn z dnia 05 kwietnia 2018 r. w sprawie powierzenia obowiązków w zakresie ochrony danych osobowych wprowadzam następujące zmiany:

1. Po § 1 Zarządzenia dodaje się § 1a w brzmieniu:
   „Do obowiązków Koordynatora ds. ochrony danych osobowych należy:
   1) Pośredniczenie w kontaktach pomiędzy pracownikami Urzędu a Inspektorem ochrony danych osobowych,
   2) Informowanie Inspektora Ochrony Danych Osobowych o zdarzeniach mogących mieć wpływ na prawidłową realizację obowiązków Inspektora,
   3) Koordynowanie wdrożenia w Urzędzie zaleceń Inspektora Ochrony Danych Osobowych
2. Dotychczasowy § 3 Zarządzenia otrzymuje brzmienie:
   „Szczegółowy zakres obowiązków Informatyka został określony w Polityce Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych obowiązujących w Urzędzie Gminy Młodzieszyn".
3. Dotychczasowy § 4 Zarządzenia otrzymuje brzmienie:
4. „Osoby dopuszczone do przetwarzania danych zobowiązuję do współpracy z Inspektorem Ochrony Danych Osobowych, Koordynatorem ds. ochrony danych osobowych oraz Informatykiem w zakresie określonym w Polityce Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych obowiązujących w Urzędzie Gminy Młodzieszyn".

§ 3

Zobowiązuję pracowników do zapoznania się z Polityką Bezpieczeństwa Danych Osobowych oraz Instrukcją Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych obowiązujących w Urzędzie Gminy Młodzieszyn, przestrzegania zasad ochrony danych osobowych oraz sposobów ich zabezpieczenia zgodnie z obowiązującymi przepisami oraz dokumentacją.

§ 4

Wykonanie zarządzenia powierzam Inspektorowi – Katarzynie Jasińskiej.

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
mgr Monika Pietrzyk