

ZARZĄDZENIE NR 2
BURMISTRZA MIROSLAWCA

z dnia 8 stycznia 2020 r.

**w sprawie wprowadzenia procedury projektowania nowych procesów w Urzędzie Miejskim
w Mirosławcu**

Na podstawie art. 24 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 (ogólne rozporządzenie o ochronie danych) zarządza się, co następuje:

§ 1. Wprowadza się „Procedurę projektowania nowych procesów w Urzędzie Miejskim w Mirosławcu” stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2. Zobowiązuje się wszystkie osoby planujące wprowadzenie nowych procesów w Urzędzie Miejskim w Mirosławcu do przestrzegania zasad i realizacji zadań określonych w załączniku, o którym mowa w § 1.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

Procedura projektowania nowych procesów w Urzędzie Miejskim w Mirosławcu

§ 1. Przedmiot i cel.

1. Niniejsza Procedura dotyczy każdego przypadku tworzenia nowego procesu związanego z przetwarzaniem danych osobowych.

2. Procedura wprowadzana jest celem wykazania, że jednostka przestrzega przepisów Rozporządzenia Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „RODO”) przyjmując środki organizacyjne, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych.

§ 2. Odpowiedzialność.

1. Nadzór nad aktualnością niniejszego dokumentu sprawuje Inspektor Ochrony Danych (IOD) przy wsparciu Administratora Systemów Informatycznych (ASI).

2. W razie wątpliwości czy potrzeby konsultacji każdy zainteresowany pracownik jednostki ma obowiązek dokonać takiej konsultacji lub wyjaśnienia wątpliwości we współpracy z IOD.

§ 3. Tryb postępowania

1. Wymaga się, aby każdy inicjator projektowanego procesu, zanim dojdzie do jego wdrożenia i przed pozyskiwaniem danych osobowych, dokonał uprzedniej konsultacji z IOD lub ASI w szczególności pod kątem:

- 1) ustalenia rodzaju przetwarzanych danych osobowych,
- 2) ustalenia kategorii osób, których te dane dotyczą,
- 3) ustalenia celów przetwarzania danych osobowych,
- 4) potwierdzenia posiadania właściwej podstawy prawnej wynikającej z RODO do przetwarzania danych w ww. celach,
- 5) w przypadku konieczności stosowania klauzul z zakresu ochrony danych osobowych – opracowania i wdrożenia ich treści,
- 6) ustalenia miejsc przetwarzania danych osobowych,
- 7) potwierdzenia, że zabezpieczenia danych osobowych są adekwatne do zagrożeń,
- 8) w przypadku wykorzystywania systemu informatycznego służącego do przetwarzania danych osobowych – uzupełnienia i pozyskania wszystkich niezbędnych informacji dotyczących przygotowania technicznych środków zabezpieczeń, na podstawie pytań określonych w § 5,

2. W każdym przypadku projektowania nowego procesu należy wziąć pod uwagę i zdefiniować proces biorąc pod uwagę w szczególności następujące kryteria:

- 1) ilość zbieranych danych osobowych,
- 2) okres ich przechowywania,
- 3) dostępność,
- 4) minimalizacja przetwarzania danych osobowych, rozumiana jako zbieranie danych osobowych wyłącznie w takim zakresie, jaki jest niezbędny do realizowania zakładanych celów; w przypadku sporządzania kopii dokumentów (np. dowodów tożsamości) zwraca się uwagę na duże ryzyko naruszenia tej zasady, dlatego pracownicy zobowiązani są do powstrzymania się od utrwalania na kopii (papierowych bądź elektronicznych) danych osobowych w nadmiernym, nieadekwatnym zakresie,
- 5) jak najszybsza pseudonimizacja danych osobowych, gdzie to zasadne, rozumiana jako przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane

dotyczą, bez użycia dodatkowych informacji; warunkiem jest przechowywanie takich dodatkowych informacji osobno i zabezpieczenie ich w ten sposób, że niemożliwe jest przypisanie ich zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej,

- 6) przejrzystość co do funkcji i przetwarzania danych osobowych, co należy rozumieć jako zdefiniowanie i ustalenie roli danych osobowych dla procesu, jak też samych procesów przetwarzania (jak zbieranie, przechowywanie, udostępnianie, usuwanie, modyfikowanie, utrwalanie),
- 7) umożliwienie osobie, której dane dotyczą, monitorowania przetwarzania danych, co w szczególności oznacza zapewnienie poszanowania praw, które dotyczą danej osoby i wynikają z RODO, jak: prawo dostępu do treści danych i posiadania ich kopii, prawo do bycia zapomnianym (usunięcie danych), prawo do przenoszenia danych, prawo do wniesienia sprzeciwu, prawo do odwołania zgody na przetwarzanie danych,
- 8) umożliwienie administratorowi tworzenia i doskonalenia zabezpieczeń, w szczególności w przypadkach zmian (organizacyjnych, lokalowych, technicznych),
- 9) nadanie przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

§ 4. Skutki procedury.

1. Podjęcie decyzji o wdrożeniu projektowanego procesu jest zawsze w gestii Administratora Danych Osobowych.

2. Wdrożenie niniejszej Procedury skutkuje tym, że podjęcie takiej decyzji powinno być dokonane w oparciu o uprzednio:

- 1) przeprowadzoną analizę procesu, zgodnie z założeniami Procedury,
- 2) sformułowane wnioski wynikające z ww. analizy,
- 3) opinię przedstawioną przez IOD lub dodatkowo ASI.

§ 5. Wymagania dla systemu informatycznego służącego do przetwarzania danych osobowych biorąc pod uwagę wymagania RODO.

1. Wymagania dotyczące uwierzytelniania

Jeżeli w systemie do logowania służy identyfikator i hasło, wymagania są następujące:

Lp.	Określenie wymogu	Czy wymóg spełniony	
		TAK	NIE
1.	System rejestruje dla każdego użytkownika odrębny identyfikator		
2.	Identyfikator użytkownika, który utracił uprawnienia, nie jest przydzielany innej osobie		
3.	Hasło do systemu informatycznego składa się co najmniej z 8 znaków		
4.	Hasło do systemu informatycznego składa się z małych i wielkich liter oraz cyfr lub znaków specjalnych		
5.	System nie posiada funkcji zapamiętania hasła, która umożliwi dostęp do systemu bez konieczności ponownego wprowadzania hasła		

2. Wymagania dotyczące funkcjonalności systemu

Lp.	Określenie wymogu	Czy wymóg spełniony	
		TAK	NIE
1.	System zapewnia automatycznie odnotowanie daty pierwszego wprowadzenia danych do systemu		
2.	System zapewnia automatycznie odnotowanie daty modyfikacji danych w systemie		

3.	System zapewnia automatycznie odnotowanie daty usunięcia danych w systemie		
4.	System zapewnia automatycznie odnotowanie identyfikatora użytkownika wprowadzającego dane do systemu		
5.	System zapewnia automatycznie odnotowanie identyfikatora użytkownika modyfikującego dane w systemie		
6.	System zapewnia automatycznie odnotowanie identyfikatora użytkownika usuwającego dane w systemie		
7.	System zapewnia odnotowanie źródła danych, jeżeli dane pochodzą nie od osoby, której dotyczą, np. zbierane są z CEIDG, zakup bazy danych - automatycznie lub ręcznie przez użytkownika		
8.	System zapewnia odnotowanie informacji o odbiorcach, którym dane zostały udostępnione - automatycznie lub ręcznie przez użytkownika [Odbiorcami, których nie dotyczy odnotowanie udostępnienia są: osoby, których dane dotyczą, osoby upoważnione do przetwarzania danych (zwłaszcza pracownicy), podmioty, z którymi podpisano umowy powierzenia (dostawcy usług - procesorzy), organy publiczne (państwowe lub organy samorządu terytorialnego), którym dane są udostępniane na podstawie przepisów prawa (np. ZUS, US, sądy, prokuratura, Policja, komornik). Odbiorcą może być np. ubezpieczyciel]		
9.	System zapewnia odnotowanie informacji o dacie udostępnienia danych odbiorcom, którym dane zostały udostępnione - automatycznie lub ręcznie przez użytkownika		
10.	System zapewnia odnotowanie informacji o zakresie danych, które zostały udostępnione odbiorcom - automatycznie lub ręcznie przez użytkownika		
11.	System zapewnia odnotowanie, jaka zgoda została wyrażona (np. wydzielenia pola przy rekordzie w systemie z opisem, czego zgoda dotyczy) - automatycznie lub ręcznie przez użytkownika		
12.	System zapewnia odnotowanie, kiedy dana zgoda została wyrażona - automatycznie lub ręcznie przez użytkownika		
13.	System zapewnia odnotowanie, kiedy dana zgoda została odwołana - automatycznie lub ręcznie przez użytkownika		
14.	System zapewnia odnotowanie informacji o dacie wniesienia sprzeciwu wobec przetwarzania danych osobowych - automatycznie lub ręcznie przez użytkownika		
15.	System zapewnia edycję danych (ich aktualizację)		
16.	System zapewnia możliwość przetwarzania danych w formie ich archiwizacji		
17.	System zapewnia możliwość trwałego usunięcia danych		
18.	System zapewnia możliwość odnotowania, że osoba, której dane dotyczą, wniosła o ograniczenie ich przechowywania (tzn. wyłącznie do ich przechowywania)		
19.	System umożliwia dostarczenie osobie, której dane dotyczą, jej własnych danych osobowych, w powszechnie używanym, ustrukturyzowanym formacie nadającym się do odczytu maszynowego		
20.	System umożliwia przesłanie danych osobowych konkretnej osoby bezpośrednio podmiotowi, któremu ona wskaże, w powszechnie używanym, ustrukturyzowanym formacie nadającym się do odczytu		

	maszynowego		
--	-------------	--	--

3. Wymagania dotyczące zabezpieczenia technicznego i fizycznego

Lp.	Określenie wymogu	Czy wymóg spełniony	
		TAK	NIE
1.	Baza danych systemu jest szyfrowana		
2.	Dostęp do danych osobowych jest zabezpieczony poprzez pseudonimizację (użycie w miejsce jednego atrybutu np. rzeczywistego imienia i nazwiska, innego atrybutu (np. inicjału, liczby), by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Te dodatkowe informacje powinny być przechowywane osobno i objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie określonej osobie fizycznej), np. szyfrowanie kluczem tajnym, funkcja skrótu, tokenizacja)		
3.	Dyski urządzeń przenośnych z zapisem danych osobowych są szyfrowane		
4.	Możliwe jest zablokowanie urządzenia lub usunięcie jego zawartości - na odległość, w razie zgubienia lub utraty		
5.	Tworzone są kopie zapasowe		
6.	Zapis kopii zapasowych danych nie jest przechowywany w pomieszczeniu, gdzie znajduje się serwer, z którego one pochodzą		
7.	Zapewnia się poufność danych przetwarzanych w systemie		
8.	Zapewnia się integralność danych przetwarzanych w systemie		
9.	Zapewnia się dostępność danych przetwarzanych w systemie		
10.	Zapewnia się odporność systemu na zagrożenia wpływające w szczególności na utratę, zabranie, nieuprawnione ujawnienie lub modyfikację, uszkodzenie danych		
11.	Zapewnia się zdolność do szybkiego przywracania dostępności danych osobowych i dostępu do nich w razie incydentu		
12.	Stosuje się regularne testowanie, mierzenie i ocenianie skuteczności zabezpieczeń systemu		
13.	Serwer, na którym przetwarzane są dane osobowe przechowywany jest w miejscu fizycznie zabezpieczonym przed utratą danych spowodowaną np. pożarem, zalaniem, włamaniem		
14.	Nośniki kopii zapasowych, na których przetwarzane są dane osobowe przechowywane są w miejscu fizycznie zabezpieczonym przed utratą danych spowodowaną np. pożarem, zalaniem, włamaniem		
15.	Komputery, na których przetwarzane są dane osobowe przechowywane są w miejscu fizycznie zabezpieczonym przed utratą danych spowodowaną np. pożarem, zalaniem, włamaniem, nieuprawnionym wglądem, kradzieżą		
16.	Każdy użytkownik posiada odrębne login+hasło do swojego konta (zarówno w przypadku profili na komputerze, jak i dedykowanych systemach informatycznych)		