Regulamin przetwarzania danych osobowych

Rady Miasta Działdowa

I. Zakres i cel Regulaminu

Na podstawie 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) wprowadza się „Regulamin przetwarzania danych osobowych w **Radzie Miasta Działdowo"**

Celem niniejszego dokumentu jest zapewnienie większego bezpieczeństwa danych osobowych oraz pozostałych informacji przetwarzanych w **Radzie Miasta Działdowo**

Regulamin przetwarzania danych osobowych w **Radzie Miasta Działdowo** określa zasady ochrony danych osobowych oraz obowiązki związane z ochroną danych osobowych w tym zakresie i jest przejawem realizacji zasady rozliczalności określonej w art. 5 ust. 2 RODO, stanowi wyciąg z Polityki Bezpieczeństwa Danych Osobowych w Urzędzie Miasta Działdowo, z którą można zapoznać się w dowolnym momencie w siedzibie Administratora Danych – Burmistrza Miasta Działdowo.

Regulamin obejmuje swoim zakresem wszystkich **Radnych Rady Miasta Działdowo**, wykonujących czynności związane z realizacją zadań jako **Rada Miasta Działdowo - Organ Kolegialny** oraz jako **Radny/Radna - osobny Administrator**, dla danych pozyskiwanych bezpośrednio od osób, których dane dotyczą.

Podstawowe pojęcia

Ilekroć w regulaminie jest mowa o:

1. Administratorze - należy przez to rozumieć Radę Miasta Działdowo/Radnego/Radną, jako osobny Administrator
2. Danych osobowych - należy przez to rozumieć wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); 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 lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3. Przetwarzaniu danych osobowych - należy przez to rozumieć 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; przetwarzanie danych osobowych obejmuje w szczególności: pozyskiwanie zgód, rozliczanie wniesionych wkładów, przechowywanie dokumentacji.
4. RODO - należy przez to rozumieć rozporządzenie 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.U. UE. L. Nr 119, s. 1 ze zm.);
5. Zgodzie - należy przez to rozumieć zgodę, o której mowa w art. 4 pkt 11) RODO, tj. 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.

II Upoważnienia do przetwarzania danych:

Radni w zakresie swojego działania, podejmują czynności w istocie jako administrator. Nie ma konieczności udzielania im upoważnień do przetwarzania danych osobowych zgodnie z art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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 z 2016 r. 119, s. 1) – dalej RODO.

III Obowiązki Administratora

1. Zapewnienie ochrony danych osobowych, osób których dane są przetwarzane przez Administratora.
2. Wprowadzenie dokumentacji dotyczącej ochrony danych osobowych oraz analiza środków technicznych i organizacyjnych w zakresie bezpieczeństwa danych oraz bieżąca współpraca z IODO
3. Zapewnienie szkolenia z zakresu ochrony danych osobowych dla Rady Miasta, co najmniej raz w roku.

IV Obowiązki Administratora Systemu Informatycznego

Role Administratora Systemów Informatycznych pełni ASI Urzędu Miasta Działdowo. Obowiązki ASI określa Polityka Bezpieczeństwa Danych Osobowych UM Działdowo.

V Gromadzenie danych osobowych

Dane osobowe przetwarzane przez Administratora mogą być uzyskiwane tylko na podstawie warunków określonych w artykule 6 ustęp 1 RODO: na podstawie zgody, zawartej umowy, do wypełnienia obowiązku prawnego, do ochrony żywotnych interesów osoby, są niezbędne do wykonania zadania realizowanego w interesie publicznym, niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora.

VI Wykorzystywanie danych

Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane przez czas wskazany w przepisach prawa.
W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.
Jeżeli dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

VII Obowiązek informacyjny

Administrator zobowiązany jest poinformować osoby, których dane osobowe przetwarza, o:

1. tożsamości i danych kontaktowych Administratora Danych Osobowych;
2. kontakt do osoby, z którą można kontaktować się w sprawach związanych z ochroną danych osobowych;
3. celach przetwarzania danych osobowych lub prawnie uzasadnionych interesach realizowanych przez administratora;
4. informacjach o odbiorcach i kategoriach odbiorców, jeżeli istnieją;
5. okresie bądź kryteriach ustalania okresu przechowywania danych osobowych
6. prawie wglądu do treści swoich danych oraz możliwości ich sprostowania, usunięcia, ograniczenia przetwarzania lub prawie do wniesienia sprzeciwu wobec przetwarzania danych oraz o prawie do przenoszenia danych;
7. w przypadku wyrażenia zgody na przetwarzanie danych osobowych o możliwości jej cofnięcia;
8. prawie do wniesienia skargi do organu nadzorczego;
9. dobrowolności bądź wymogu ustawowym podania danych osobowych oraz o konsekwencjach niepodania danych.

W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy dodatkowo poinformować o źródle danych oraz o uprawnieniach wynikających z art. 14 Rozporządzenia. W celu realizacji obowiązku informacyjnego stosuje się klauzule informacyjne, które powinny być umieszczone w siedzibie Administratora.

VIII Zgody na przetwarzanie danych osobowych

Jeżeli przetwarzanie odbywa się na podstawie zgody na przetwarzanie danych osobowych, administrator dba, aby zgody były wyrażane dobrowolnie oraz żeby były zrozumiałe.
W przypadku zbierania zgód należy poinformować osobę o możliwości jej wycofania.

IX Udostępnienie danych osobowych

Administrator udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
Dane osobowe mogą być udostępniane w następujących przypadkach:

1. na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;
2. na podstawie umowy z innym podmiotem, w ramach, której istnieje konieczność udostępnienia danych;
3. na podstawie wniosku osoby, której dane dotyczą.

Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje niezwłocznie.

X Odmowa udostępnienia danych

Odmowa udostępnienia danych osobowych następuje na podstawie obowiązków wynikających z art. 32 dotyczących bezpieczeństwa przetwarzania danych osobowych. Wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

XI Obowiązki podmiotu przetwarzającego i powierzenie danych

Powierzenie przetwarzania danych osobowych podmiotowi przetwarzającemu odbywa się zgodnie z art. 28 RODO na podstawie umowy zawartej na piśmie pomiędzy Administratorem a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.

XII Postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych

Zasady postępowania w przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.
Przypadki naruszenia bezpieczeństwa danych osobowych
Naruszeniem bezpieczeństwa danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
1) nieautoryzowany dostęp do danych;
2) nieautoryzowane modyfikacje lub zniszczenie danych;
3) udostępnienie danych nieautoryzowanym podmiotom;

4) nielegalne ujawnienie danych;
5) pozyskiwanie danych z nielegalnych źródeł.

Postępowanie w razie wykrycia naruszeń
W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych (w przypadku ataku z sieci - odłączyć komputer od zasilania) i niezwłocznie powiadomić o tym fakcie Administratora Danych Osobowych, następnie postępować stosownie do podjętej przez niego decyzji.
Zgodnie z art. 33 Rozporządzenia po przeprowadzonej analizie przypadku naruszenia oraz możliwych konsekwencji wystąpienia naruszenia dla praw i wolności osób fizycznych ADO opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości;

Do analizy ryzyka naruszenia praw lub wolności osób fizycznych stosuje się metodę oceny wagi naruszenia Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)
WN = KPD * PI + ON
• Waga Naruszenia - WN
• Kontekst Przetwarzania Danych - KPD – główny czynnik określający poziom krytyczności zestawu naruszonych danych, w określonym kontekście przetwarzania.
• Prawdopodobieństwo Identyfikacji - PI – czynnik korygujący KPD, który może obniżyć wynik. Prawdopodobieństwo (łatwość) identyfikacji osoby na podstawie naruszonych danych dla osób, które uzyskały dostęp do nich.
• Okoliczności Naruszenia - ON – czynnik, który odnosi się do okoliczności naruszenia, które wystąpiły lub nie w danym przypadku.
Na podstawie raportu Administrator podejmuje decyzje czy:
1) Należy zgłosić naruszenie ochrony danych osobowych organowi nadzorczemu;
2) Należy zawiadomić osoby, których dane zostały naruszone.
Zgłoszenia oraz zawiadomienia, o których mowa powyżej winny być zrealizowane niezwłocznie nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia.
Zgłoszenie do Urzędu Ochrony Danych Osobowych odbywa się na udostępnionym formularzu przez Prezesa znajdującym się na stronie uodo.gov.pl.

XIII Rejestr czynności przetwarzania.

Rejestr czynności przetwarzania Rady Miasta Działdowo stanowi integralną część Rejestru czynności Urzędu Miasta Działdowo.

XIV Rejestr wszystkich kategorii czynności przetwarzania

W sytuacji, gdy jednostka staje się podmiotem przetwarzającym na polecenie innych administratorów danych, sytuacja ta jest odnotowywana w prowadzonym wewnętrznie rejestrze wszystkich kategorii czynności. Rejestr prowadzony jest zgodnie z obowiązkiem wynikającym z art. 30 rozporządzenia, rejestr jest udostępniany na żądanie organu nadzorczego.

XV Przetwarzanie i ochrona danych osobowych w systemach informatycznych

1. Osobą nadzorującą przestrzeganie zasad ochrony danych osobowych przetwarzanych w systemach informatycznych jest Administrator Systemów Informatycznych (ASI).
2. Dane osobowe zawarte w systemach informatycznych mogą być przetwarzane jedynie przez osoby upoważnione do przetwarzania danych osobowych zgodnie z zasadami niniejszego Regulaminu.
3. Przed dostępem osób nieupoważnionych, dane osobowe przetwarzane w systemach informatycznych są zabezpieczone przed otwarciem hasłem.
4. Hasła do zabezpieczonych danych osobowych znane są tylko upoważnionym do przetwarzania danych osobom. Hasła muszą być silne, złożone z co najmniej 8 znaków, zawierających liczby, litery i znaki specjalne. Zabrania się pracownikom udostępniania haseł osobom trzecim. Zabrania się korzystania przez pracowników z haseł innych osób.
5. Wszystkie komputery zabezpieczone są w licencjonowane oprogramowanie antywirusowe, podlegające aktualizacji. Programy antywirusowe zainstalowane są na stacjach roboczych. Po każdej naprawie i konserwacji komputera sprzęt jest sprawdzany pod kątem występowania wirusów i konieczności ponownego zainstalowania programu antywirusowego. Elektroniczne nośniki informacji pochodzenia zewnętrznego podlegają automatycznemu sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich.
6. Dane uzyskiwane drogą teletransmisji podlegają sprawdzeniu przed udostępnieniem użytkownikom.
7. W zakresie korzystania z sieci komputerowej obowiązują następujące zasady:
- pracownicy nie są uprawnieni do instalacji jakiegokolwiek prywatnego oprogramowania bez odpowiedniej zgody ADO. W przypadku zainstalowania takiego oprogramowania bez odpowiedniej akceptacji pracownik ponosi odpowiedzialność porządkową i prawną,
- oprogramowanie na komputerach może być zainstalowane wyłącznie przez ADO lub innego upoważnionego pracownika,
- pracownicy mogą używać połączenia z Internetem jedynie w celach służbowych, jedynie z przeznaczonych do tego celu komputerów,
- pracownicy nie mają prawa przekazywać za pośrednictwem sieci komputerowej do stron trzecich jakichkolwiek danych,
- pracownicy nie mogą ściągać za pośrednictwem sieci komputerowej żadnego nielegalnego lub pirackiego oprogramowania,
- pracownicy nie mogą podłączać się do sieci zewnętrznej za pośrednictwem modemów lub sieci wi-fi.
8. W trakcie pracy z wykorzystaniem systemu komputerowego obowiązuje przestrzeganie następujących zasad:
- należy w miarę możliwości, ustawiać monitor komputerowy w taki sposób, aby informacje na ekranie nie były widoczne dla osób postronnych,
- zawsze należy stosować hasła dostępu,
- przy opuszczaniu stanowiska pracy należy wylogować się z systemu (Windows +L)
- wszelkie usterki należy zgłaszać ADO.
9. W każdym wypadku współpracy z innymi podmiotami, zarówno w zakresie importu danych do programów, jak i udostępniania danych zawartych w tych programach, obowiązuje najwyższy poziom zabezpieczenia tego dostępu.

Radnym Rady Miasta Działdowo

- zabrania się:

1. Przechowywania haseł w miejscu widocznym bądź łatwo dostępnym dla innych osób,
2. Zapisywania haseł w pamięci komputera,
3. Udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
4. Udostępniania osobom nieuprawnionym programów komputerowych zainstalowanych w systemie,
5. Używania programów w innym zakresie niż pozwala na to umowa licencyjna,
6. Przenoszenia oprogramowania z jednego stanowiska na inne bez wiedzy i zgody ASI lub osoby przez niego upoważnionej,
7. Wymontowania bądź przenoszenia dysków twardych z jednego stanowiska na inne,
8. Tworzenia kopii danych na zewnętrznych nośnikach w celu wyniesienia ich poza obszar przetwarzania bez zgody ASI lub osoby przez niego upoważnionej,
9. Instalowania i używania jakichkolwiek programów komputerowych (w tym również programów do użytku prywatnego) bez wiedzy i zgody ASI lub osoby przez niego upoważnionej,
10. Używania zewnętrznych nośników danych bez wcześniejszego sprawdzania programem antywirusowym.
11. Przechowywania danych osobowych na zewnętrznych nośnikach bez ich stosownego zabezpieczenia hasłami lub szyfrowania.
12. Pozostawiania dokumentów na biurku po zakończonej pracy, pozostawiania otwartych dokumentów na ekranie monitora bez blokady dostępu,
13. Pozostawiania dokumentów bądź kopii dokumentów zawierających dane osobowe w drukarkach bądź kserokopiarkach,
14. Wyrzucania dokumentów zawierających dane osobowe bez uprzedniego trwałego zniszczenia,
15. Pozostawiania osób trzecich bez nadzoru w pomieszczeniach, w których przetwarzane są dane osobowe,
16. Przekazywania danych osobowych osobom nieupoważnionym
17. Przesyłania niezaszyfrowanych dokumentów z danymi osobowymi z wykorzystaniem konta pocztowego
18. Ignorowania zapisów Regulaminu.

- **wymagane jest:**

1. Posługiwanie się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych,
2. Tworzenie haseł trudnych do odgadnięcia dla innych użytkowników oraz osób nieupoważnionych,
3. Zabezpieczanie hasłem/szyfrowanie wszystkich plików, które zawierają dane osobowe,
4. Zabezpieczenie sprzętu komputerowego w tym komputerów przenośnych przed kradzieżą lub nieuprawnionym dostępem do danych.
5. Osoby przetwarzające informacje zawierające dane osobowe zobowiązane są do zachowania tajemnicy służbowej.
6. Osoby przetwarzające informacje zawierające dane osobowe zobowiązane są do niezwłocznego poinformowania Administratora o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.
7. Przed wysłaniem pliku zawierającego dane osobowe należy go odpowiednio zabezpieczyć poprzez zaszyfrowanie hasłem. Hasło należy przesłać odbiorcy pliku inną drogą komunikacji.
8. Każdy pracownik jest zobowiązany do zgłaszania naruszeń ochrony danych - niezwłocznie do bezpośredniego przełożonego.
9. Zgłaszanie naruszeń ochrony danych.

Procedura obowiązuje od dnia 12.08.2024 r.

Lista osób, które otrzymały i zapoznały się z **Regulaminem ochrony danych osobowych przetwarzanych w Rady Miasta Działdowo**

Imię i nazwisko	**Stanowisko**	**Data zapoznania się z Regulaminem**	**Podpis**