Załącznik Nr 1 do zarządzenia Nr 14/2024

Wójta Gminy Dragacz

z dnia 9 lutego 2024 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI w Urzędzie Gminy Dragacz

Rozdział 1. POSTANOWIENIA OGÓLNE

§ 1. Niniejsza polityka została opracowana na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO)(Dz.Urz.UE L119 z 4 maja 2016 r.).

§ 2. Użyte w niniejszej polityce wyrażenia oznaczają:

1) **Administrator** (**ADO**) - organ, jednostka organizacyjna, podmiot lub osoba decydujące o celach i środkach przetwarzania danych osobowych. Administratorem jest Gmina Dragacz, reprezentowana przez Wójta Gminy;
2) **Inspektor Ochrony Danych (IOD)** - osoba fizyczna upoważniona przez Administratora, zajmująca się nadzorowaniem przestrzegania przepisów o ochronie danych osobowych oraz prowadzeniem wymaganej prawem dokumentacji związanej z przetwarzaniem tych danych przez administratora;
3) **baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci wewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze – rekordów lub obiektów, w których są zapisywane dane osobowe;
4) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne;
5) **droga elektroniczna** – poczta elektroniczna lub elektroniczna skrzynka podawcza, o której mowa w art. 3 pkt 17 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2023 r. poz. 57 z późn. zm.);
6) **działanie korygujące** - działanie przeprowadzane w celu wyeliminowania przyczyny wykrytej niezgodności / incydentu lub innej niepożądanej sytuacji;
7) **działanie zapobiegawcze** - działanie, które należy przedsięwziąć, aby wyeliminować przyczyny potencjalnej niezgodności/incydentu lub innej potencjalnej sytuacji niepożądanej;
8) **PUODO –** Prezes Urzędu Ochrony Danych Osobowych;
9) **hasło** – ciąg znaków literowych, cyfrowych lub innych, uwierzytelniający osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
10) **identyfikator Użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
11) **incydent -** pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji lub zmniejszeniem poziomu usług systemowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działania systemu informatycznego i zagrażają bezpieczeństwu informacji; naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność;
12) **informacja stanowiąca tajemnicę służbową -** informacja uzyskana w związku z czynnościami służbowymi lub wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli, interesu publicznego lub Gminy Dragacz;

13) **Administrator Systemów Informatycznych (ASI)** – osoba fizyczna wyznaczona przez ADO, zajmująca się sprawowaniem ogólnego nadzoru nad bezpieczeństwem organizacyjnym, fizycznym oraz technicznym danych osobowych przetwarzanych w systemie informatycznym stosowanym w Urzędzie Gminy Dragacz;

14) **IZSI –** Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Dragacz;

15) k**orekcja** - działanie w celu wyeliminowania wykrytej niezgodności lub incydentu;

16) k**ontrola (Audyt)** - systematyczny, niezależny i udokumentowany proces oceny skuteczności systemu ochrony danych osobowych, na podstawie określonych kryteriów, wymagań polityk i procedur;

17) n**iezgodność** - niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe;

18) n**ośniki danych** – przedmioty fizyczne (elektroniczne, papierowe), na których możliwe jest zapisanie informacji w celu ich przechowywania, przetwarzania i transmisji. Każdy nośnik danych charakteryzuje określona gęstość zapisu, wynikająca z jego właściwości fizycznych;

19) o**dbiorca danych** – każdy, komu udostępniane są dane osobowe, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela administratora danych mającego siedzibę w państwie trzecim, przetwarzającego dane przy wykorzystaniu środków technicznych znajdujących się na terytorium RP, podmiotu który przetwarza dane na podstawie umowy powierzenia zawartej z administratorem, a także organów państwowych i organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

20) p**odatność** - luka (słabość), która może być wykorzystana przez co najmniej jedno zagrożenie, rozumiane jako potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę.

21) **PBI / Polityka** – niniejszy dokument;

22) p**racownik** – osoba fizyczna świadcząca na rzecz Urzędu Gminy Dragacz pracę na podstawie stosunku pracy, powołania, mianowania, wykonująca zadania wyłącznie osobiście, w ramach prowadzonej działalności gospodarczej lub powierzone jej na podstawie umowy cywilnoprawnej, w rozumieniu ustawy z dnia 13 października 1998 roku o systemie ubezpieczeń społecznych (Dz.U. 2023 z 2023 r. , poz. 1230 z późn. zm);

23) p**rzetwarzane danych** – wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemie informatycznym;

24) s**łabość systemu** - zdarzenie, stan rzeczy zwiększający ryzyko wystąpienia incydentu;

25) **Urząd** – Urząd Gminy Dragacz z siedzibą przy ul. Dragacz 7a;

26) s**ystem informatyczny (system IT)** - zespół współpracujących ze sobą urządzeń, programów, systemów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

27) s**ystem tradycyjny** - zespół procedur organizacyjnych, wyposażenia i środków trwałych związanych z mechanicznym przetwarzaniem informacji zawierających dane osobowe na nośnikach papierowych;

28) s**erwisant** – pracownik firmy zewnętrznej lub pracownik Urzędu Gminy Dragacz w rozumieniu ust. 22 niniejszego paragrafu zajmujący się instalacją, naprawą i konserwacją sprzętu komputerowego;

29) p**rzepisy prawa** – obowiązujące przepisy w zakresie ochrony danych osobowych;

30) s**ieć publiczna** – sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;

31) s**ytuacja kryzysowa** - sytuacja wpływająca negatywnie na poziom bezpieczeństwa zasobów i infrastruktury technicznej, każde zdarzenie, zagrożenie lub domniemanie utraty poufności, integralności lub dostępności informacji wrażliwej przetwarzanej w systemie teleinformatycznym;

32) t**eletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

33) u**suwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą;

34) u**wierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

35) u**żytkownik** – pracownik Urzędu Gminy Dragacz bez względu na rodzaj stosunku pracy i wymiar etatu, stażysta, praktykant oraz każda inna osoba, która uzyskała upoważnienie od ADO do przetwarzania danych osobowych w systemach IT;

36) z**abezpieczenie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

37) z**agrożenie** - potencjalna możliwość wystąpienia incydentu;

38) z**biór danych osobowych** - posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

39) z**darzenie** - błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z zagrożeniem bezpieczeństwa danych osobowych;

40) p**rocesor** - podmiot zajmujący się przetwarzaniem danych osobowych, które powierzył mu ADO. Procesorem może być osoba fizyczna, prawna, organ publiczny, jednostka lub inny podmiot;

41) **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

§ 3. 1. PBI jest wewnętrznym dokumentem regulującym zasady przetwarzania i ochrony danych osobowych w Urzędzie.

2. PBI została opracowana i wdrożona w celu uzyskania standardu przetwarzania informacji zawierających dane osobowe zgodnego z wymaganiami określonymi w przepisach prawa, o których mowa w § 1 niniejszego dokumentu, w szczególności danych osobowych przetwarzanych w systemie informatycznym wykorzystywanym w Urzędzie oraz pozostałych informacji podlegających ochronie.

3. Niniejszy dokument winien być udostępniony każdej osobie mającej dostęp do danych osobowych przetwarzanych w Urzędzie.

§ 4. 1. PBI określa w szczególności:

1) prawa, obowiązki oraz granice dopuszczalnego zachowania osób przetwarzających dane osobowe w związku z działalnością Gminy, Użytkowników systemów IT i tradycyjnych, w których przetwarzane są dane osobowe oraz konsekwencje naruszenia przepisów o ochronie danych osobowych wymienionych w § 1.;

2) sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę tych danych, w tym podstawowe warunki jakim powinny odpowiadać urządzenia z wykorzystaniem których dane są przetwarzane;

3) wymagania w zakresie odnotowywania udostępniania danych osobowych;

4) instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych.

2. Zastosowane zabezpieczenia mają zapewnić:

1) poufność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobom;

2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

3) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;

4) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji zamierzonej, jak i przypadkowej;

5) dostępność informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;

6) zarządzanie ryzykiem - rozumiane jako proces identyfikowania, monitorowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa informacji, które może dotyczyć systemów informatycznych i tradycyjnych służących do przetwarzania danych osobowych.

Rozdział 2.
Administrator. Inspektor Ochrony Danych Osobowych. Administrator Systemów Informatycznych

§ 5. 1. ADO podejmuje decyzje w zakresie realizacji celów i zapewnienia środków zapewniających bezpieczeństwo przy przetwarzaniu danych osobowych, zgodnie z wymogami i zaleceniami wynikającymi z przepisów prawa w celu ochrony interesów osób, których dane dotyczą.

2. ADO pełni funkcję kontrolną w zakresie poprawnego przetwarzania danych osobowych oraz nadzoruje przestrzeganie ustalonych zasad zawartych w PBI.

3. ADO jest zobowiązany do zgłoszenia wyznaczenia IOD. W przypadku niepowołania IOD, funkcje mu przypisane ADO pełni w zakresie zgodnym z obowiązującymi przepisami.

4. Zadania nałożone na ADO przez RODO:

1) wypełnianie obowiązku informacyjnego przy zbieraniu danych osobowych w tym udzielanie informacji o celu i zakresie przetwarzanych danych osobowych;
2) dochowanie szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane przetwarza;
3) obowiązek uzupełniania, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane;
4) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
5) nadawanie upoważnień do przetwarzania danych osobowych;
6) nadzór nad procesami przetwarzania danych;
7) obowiązek kontrolowania jakie dane, kiedy i przez kogo zostały wprowadzone do zbioru i komu są przekazywane;
8) zapewnienia bezzwłocznego włączenia IOD we wszelkie sprawy dotyczące ochrony danych osobowych – art. 38 RODO;
9) umożliwienia udziału IOD w spotkaniach przedstawicieli wyższego i średniego szczebla organizacji;
10) organizacji uczestnictwa IOD przy podejmowaniu decyzji dotyczących przetwarzania danych osobowych. Niezbędne informacje powinny zostać udostępnione IOD odpowiednio wcześniej, umożliwiając IOD zajęcie stanowiska;
11) w przypadku stwierdzenia naruszenia albo innego zdarzenia związanego z danymi osobowymi zobowiązania organizacji do natychmiastowej konsultacji z IOD.

§ 6. IOD jest wyznaczony przez ADO drogą pisemnego upoważnienia. Wzór upoważnienia dla IOD stanowi załącznik nr 3 do PBI. IOD jest również zobowiązany do podpisania oświadczenia o zachowaniu poufności (załącznik nr 2 do PBI).

§ 7. Do kompetencji IOD należy w szczególności:

1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowywanie w tym zakresie raportów dla ADO nie rzadziej niż raz na rok;
2) nadzorowanie przestrzegania zasad ochrony danych osobowych, tj. środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, ze szczególnym uwzględnieniem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w tym nadzór nad obiegiem oraz przechowywaniem materiałów i dokumentów zawierających dane osobowe we współpracy z ASI w zakresie dotyczącym systemu IT;

3) nadzorowanie opracowania i aktualizacji dokumentacji opisującej sposób przetwarzania danych, środki ich ochrony oraz przestrzegania zasad w niej określonych;

4) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

5) wyjaśnianie na wniosków dotyczących bezpieczeństwa informacji, w tym danych osobowych, a także nadzór w zakresie realizacji tych wniosków;

6) nadzór nad fizycznym zabezpieczeniem pomieszczeń we współpracy z ADO, w których przetwarzane są dane osobowe oraz organizacją kontroli przebywających w nich osób;

7) zapewnienie przeciwdziałania incydentom oraz prowadzenie rejestru zdarzeń (załącznik nr 11 do PBI);

8) w porozumieniu z ASI, szkolenie osób upoważnionych do przetwarzania danych osobowych w zakresie przepisów o ochronie danych osobowych oraz zapewnienie bieżącej edukacji Użytkowników w zakresie polityki bezpieczeństwa, w tym wnioskowanie do ADO o organizację tych szkoleń.

§ 8. 1. W ramach nadzoru nad przetwarzaniem danych, IOD sprawdza w szczególności cele, zakres przetwarzania, czas przetwarzania oraz sposoby zabezpieczenia danych osobowych w działalności Urzędu Gminy Dragacz.

2. IOD jest również zobowiązany do przeprowadzania analizy ryzyk związanych z zagrożeniami związanymi z przetwarzaniem danych osobowych w systemie informatycznym oraz tradycyjnym z uwzględnieniem specyfiki pracy wiążącej się z koniecznością przetwarzania danych osobowych poza siedzibą ADO z wykorzystaniem urządzeń mobilnych.

§ 9. 1. Do zadań ASI należy zapewnienie działania infrastruktury teleinformatycznej i oprogramowania w sposób zapewniający właściwy poziom bezpieczeństwa informacji wynikający z obowiązujących przepisów, PBI oraz zaleceń IOD.

2. Nadzorowanie przez ASI przestrzegania bezpieczeństwa danych osobowych gromadzonych i przetwarzanych w systemach IT ma na celu zabezpieczenie ich przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem

3. Do kompetencji ASI należy w szczególności:

1) zapewnienie właściwego poziomu bezpieczeństwa systemu informatycznego, w tym danych osobowych w nich przetwarzanych;

2) zapewnienie mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrola dostępu do danych osobowych;

3) inicjatywa w zakresie zapewnienia alternatywnego, awaryjnego zasilania systemu informatycznego oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych, w tym raportowanie do IOD stanu zabezpieczeń w zakresie centralnego awaryjnego zasilania budynku;

4) podejmowanie działań zabezpieczających system informatyczny w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu, informacji o zmianach w sposobie działania systemu lub innych urządzeń wskazującej na naruszenie bezpieczeństwa danych;

5) zapewnienie ochrony systemu teleinformatycznego oraz danych osobowych przesyłanych za pośrednictwem tych systemów;

6) zapewnienie ochrony danych osobowych w związku z naprawą, konserwacją oraz likwidacją systemu informatycznego, w tym urządzeń komputerowych, na których zapisane są dane osobowe;

7) zapewnienie przeglądów, konserwacji oraz uaktualnień systemu służącego do przetwarzania danych osobowych, w tym w szczególności z uwzględnieniem specyfiki działalności Gminy.

Rozdział 3.

Zasady przetwarzania danych osobowych. Profilowanie. Powierzenie. Udostępnianie. Obowiązek informacyjny. Zgoda. Zabezpieczenia. Sprawdzenia. Odpowiedzialność

§ 10. 1. Zasady przetwarzania danych osobowych:

1) dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Gmina może żądać podania jedynie tych danych, które są niezbędne do realizacji jej celów i zadań;

2) zakres danych osobowych przetwarzanych przez jednego Użytkownika w systemie IT nie może być szerszy niż powierzony do przetwarzania w związku z wykonywanymi przez niego obowiązkami;

3) po wykorzystaniu, dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą, zniszczone lub, w przypadku powierzenia, zwrócone podmiotowi, który dane powierzył.

2. Zasady ochrony danych osobowych określone przez PBI mają zastosowanie do:

1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów przetwarzania informacji zawierających dane osobowe, w tym systemów IT;

2) informacji będących własnością Gminy oraz przetwarzanych przez nią w związku z prowadzoną działalnością;

3) wszystkich lokalizacji, budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;

4) wszystkich osób świadczących pracę lub wykonujących czynności na rzecz Gminy mających dostęp do informacji podlegających ochronie;

5) wszystkich podmiotów współpracujących z Gminą.

§ 11. Przetwarzanie danych osobowych odbywa się z wykorzystaniem dokumentów, materiałów, przesyłek analogowych (nieelektronicznych), wniosków, pism, akt osobowych pracowników, dokumentów finansowo-księgowych, podań itp. oraz danych zawartych na nośnikach elektronicznych, magnetycznych, optycznych i elektronicznych, w tym przekazywanych drogą elektroniczną, jako załączniki do przesyłek analogowych, a także danych przetwarzanych w systemie kadrowo-płacowym, systemie do obsługi dokumentów ubezpieczeniowych i wymianie informacji z ZUS, systemie teleinformatycznym administracji.

§ 12. Obszarem przetwarzania danych osobowych są wydzielone pomieszczenia lub części pomieszczeń w siedzibie Urzędu Gminy Dragacz.

§ 13. Wszystkie osoby, które posiadają dostęp do danych osobowych w obszarze wymienionym w § 12 muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez ADO lub IOD oraz podpisać oświadczenie o zachowaniu poufności. Wzór upoważnienia stanowi załącznik nr 1 do PBI. Wzór oświadczenia o zachowaniu poufności stanowi załącznik nr 2 do PBI.

§ 14. Uprawnienia do przetwarzania danych osobowych w systemach IT nadawane są zgodnie z właściwą procedurą określoną w IZSI służącym do przetwarzania danych osobowych w Urzędzie. Uprawnienia, o których mowa w zdaniu pierwszym, ważne są do dnia odwołania lub do chwili ustania zatrudnienia uprawnionego pracownika.

§ 15. 1. Ochrona dotyczy w szczególności:

1) danych osobowych gromadzonych i przetwarzanych w związku z działalnością Gminy, w tym danych osobowych podmiotów współpracujących;

2) danych osobowych pracowników, w tym danych osobowych i treści zawieranych umów o pracę**;**

3) danych osobowych kandydatów do pracy zbieranych na etapie rekrutacji**;**

4) danych osobowych zawartych w dokumentach finansowo-księgowych; informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach IT, w których są przetwarzane dane osobowe;

5) rejestru osób dopuszczonych do przetwarzania danych osobowych;

6) danych osobowych zawartych w pozostałych dokumentach wytwarzanych w związku z działalnością Gminy;

2. Katalog zbiorów przetwarzanych danych osobowych może ulec rozszerzeniu w zależności od zakresu bieżącej działalności Gminy.

§ 16. 1. W zbiorach danych gromadzonych w systemach IT zabrania się przetwarzania danych ujawniających stan zdrowia, pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, przynależność partyjną lub związkową, dane genetyczne, dane biometryczne, nałogi, preferencje seksualne, chyba że wymagają tego obowiązujące przepisy prawa lub osoba, której dane dotyczą, wyraziła na to pisemną zgodę.

2. Dane o skazaniach, w tym dane o niekaralności można przetwarzać wyłącznie w zakresie uregulowanym w art. 6 ust. 1 pkt 10 ustawy z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz.U. z 2023 r. poz.1068 z późn. zm.).

§ 17. 1. Do przetwarzania powierzonych danych osobowych mogą być dopuszczeni jedynie pracownicy oraz pracownicy podmiotów współpracujących lub świadczących usługi na rzecz Gminy (procesorów, podmiotów współpracujących) w zakresie adekwatnym do celu powierzenia.

2. Powierzenie przetwarzania danych osobowych następuje na podstawie umowy powierzenia lub innego aktu prawnego, zawartej w formie pisemnej lub dopuszczalnej prawem formie elektronicznej (oświadczenie złożone drogą elektroniczną lub zapisane na elektronicznym nośniku informacji, określona opcja internetowa). Wzór umowy powierzenia, zgodny z art. 28 rozporządzenia ogólnego (RODO), stanowi załącznik nr 10 do PBI.

3. Umowa powierzenia danych osobowych określa przedmiot i czas trwania przetwarzania, zakres, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, obowiązki i prawa stron umowy (administratora i procesora).

4. Podmiot, z którym zostaje zawarta umowa powierzenia jest zobowiązany do wdrożenia środków organizacyjnych i technicznych odpowiednich do ryzyk przetwarzania powierzonych danych, prowadzenia rejestru czynności przetwarzania, zgłaszania naruszeń ochrony danych do organu nadzorczego, czyli PUODO

5. W przypadku, w którym podmiot określony w umowie powierzenia danych osobowych, w zakresie realizacji swoich usług korzysta z pomocy innych podmiotów (podpowierzenie danych), wymagana jest szczegółowa lub ogólna zgoda ADO na przekazanie powierzonych danych, wyrażona w formie pisemnej lub równoważnej jej formie elektronicznej.

6. IOD jest zawiadamiany o każdej umowie co do której zachodzi prawdopodobieństwo powierzenia danych, w rozsądnym terminie celem przygotowania lub akceptacji umowy powierzenia przetwarzania.

§ 18. 1. Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie w sytuacji, w której administrator danych udostępniający dane oraz administrator danych pozyskujący dane drogą udostępnienia posiadają odpowiednią podstawę prawną w sprawie ww. czynności.

2. ADO może odmówić udostępnienia danych osobowych w sytuacji, w której spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób oraz w sytuacji, w której dane osobowe nie mają istotnego związku ze wskazanymi motywami działania wnioskującego o udostępnienie danych.

3. W przypadku konieczności udostępniania dokumentów i danych w nich zawartych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych.

4. W przypadku, gdy dane osobowe osoby, od której zostały zebrane, są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem przepisów prawa lub są zbędne do realizacji celu, dla którego zostały zebrane, ADO lub osoba przez niego upoważniona jest zobowiązana do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

5. IOD jest zawiadamiany o każdym przypadku udostępnienia danych celem akceptacji.

§ 19. 1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, ADO jest obowiązany poinformować tę osobę o:

1) adresie swojej siedziby i pełnej nazwie;

2) celu i zakresie zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych;

3) dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej i konsekwencjach niepodania danych;

4) Inspektorze Ochrony Danych Osobowych;

5) prawnie uzasadnionym interesie administratora, jeżeli na tej podstawie odbywać się będzie przetwarzanie danych;

6) okresie, przez który dane osobowe będą przechowywane lub o kryteriach tego okresu;

7) profilowaniu danych;

8) prawach osoby, której dane dotyczą, tj. prawie do usunięcia danych, ograniczenia przetwarzania, przenoszenia danych, cofnięcia zgody (gdy osoba, której dane dotyczą wyraża zgodę na przetwarzanie danych).

2. W przypadku pozyskania danych osobowych z innego źródła, niż osoba, której dane dotyczą, ADO jest zobowiązany poinformować tę osobę, oprócz wymienionych w ust. 1 pkt 1-8, o źródle pozyskania danych oraz uprawnieniach wynikających z RODO.

3. Obowiązek poinformowania wymieniony w ust. 1 niniejszego paragrafu powinien być wykonany w momencie zbierania danych z wyjątkiem sytuacji, w której przepis innej ustawy zezwala na przetwarzanie danych osobowych.

4. Obowiązek poinformowania wymieniony w ust. 2 niniejszego paragrafu powinien zostać spełniony bezpośrednio po utrwaleniu zebranych danych, a więc po zapisaniu danych w sposób umożliwiający ich dalsze przetwarzanie.

§ 20. 1. Zgodnie z art. 4 ust. 11 RODO, zgoda to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

2. Zgoda na przetwarzanie danych osobowych nie może być domniemana lub dorozumiana ani wynikać z oświadczenia woli o innej treści, tzn. zgoda nie może być zawarta np. w regulaminie, którego zaakceptowanie wiąże się ze zgodą na warunki w nim zawarte.

3. Zgodnie z ust. 32 preambuły RODO, w przypadku pozyskania zgody w formie innej niż pisemna, na ADO ciąży obowiązek udowodnienia, że została ona pozyskana, a nie dorozumiana – „*Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny oznaczać zgody*".

4. Zgoda na przetwarzanie danych osobowych powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, należy pozyskać odrębną zgodę na każdy cel.

5. Zgodnie z ust. 32 preambuły RODO, elektroniczne pytanie o zgodę musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.

6. Zgoda na przetwarzanie danych osobowych może być odwołana w każdym czasie w sposób tak samo prosty i przystępny, w jaki została pozyskana.

§ 21. Zgoda na przetwarzanie danych osobowych nie jest wymagana w przypadku, gdy dane będą przetwarzane:

1) w związku z zawarciem umowy z osobą, której dane dotyczą;

2) na podstawie przepisu prawa;

3) w interesie publicznym;

4) w prawnie usprawiedliwionym celu administratora danych;

5) w przypadku żywotnego interesu osoby, której dane dotyczą, gdy pozyskanie zgody jest konieczne, ale niemożliwe.

§ 22. W celu zapewnienia należytej ochrony przetwarzania danych osobowych, w Urzędzie zastosowano środki zabezpieczające powierzone zbiory danych w postaci zabezpieczeń technicznych i organizacyjnych.

§ 23. 1. Dokumenty zawierające dane osobowe w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w zabezpieczonych pomieszczeniach (zamki na klucz, karty zbliżeniowe).

2. Pomieszczenia, w których przetwarzane są dane osobowe wyposażone są w system ostrzegania alarmowego, w tym dźwiękowego.

3. Dostęp do pomieszczeń kontrolowany jest przez system całodobowego monitoringu wizyjnego.

4. W przypadku konieczności zniszczenia papierowych dokumentów zawierających dane osobowe, ich zniszczenia dokonuje się poprzez pocięcie w niszczarce.

5. Do ochrony dostępu do sieci komputerowej stosuje się zaporę sieciową Firewall.

6. Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

7. Dla potrzeb ochrony danych osobowych przetwarzanych w edytorach tekstu (Ms Word), arkuszach kalkulacyjnych (Ms Excel) lub programach równorzędnych (np. Open Office) i innych programach do tworzenia baz danych oraz w systemach informatycznych, np. Płatnik, system bankowości elektronicznej itp. stosuje się środki ochrony przed szkodliwym oprogramowaniem: robaki, wirusy, konie trojańskie itp.

8. W przypadku wystąpienia konieczności dostępu do zbioru danych osobowych w czasie nieobecności pracownika upoważnionego do przetwarzania danych w tym zbiorze, IOD, w porozumieniu z ASI w zakresie dostępu do systemu informatycznego, może udostępnić ten zbiór innemu pracownikowi w celu dokonania niezbędnych czynności służbowych. Po powrocie nieobecny pracownik otrzymuje nowe indywidualne hasło dostępu.

9. Z każdego zdarzenia opisanego w ust. 8 niniejszego paragrafu, IOD sporządza protokół, w którym podaje: imiona i nazwiska osób zastępujących nieobecnego pracownika.

10. Zastosowany system informatyczny umożliwia rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.

11. Zastosowany system informatyczny umożliwia określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego w tym systemie zbioru danych osobowych.

12. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

§ 24. 1. Opracowano i wdrożono PBI oraz Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie.

2. Powołano IOD, który sprawuje nadzór nad przetwarzaniem danych osobowych w systemie tradycyjnym.

3. Wyznaczono ASI, który sprawuje nadzór nad przetwarzaniem danych osobowych w systemie informatycznym.

4. Wszystkie osoby wykonujące czynności związane z przetwarzaniem danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony tych danych.

5. Wszyscy Użytkownicy systemu informatycznego zostali przeszkoleni w zakresie zasad korzystania i zabezpieczeń tego systemu.

6. Do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez ADO oraz które podpisały oświadczenie o zachowaniu poufności zobowiązujące je do zachowania przetwarzanych danych w tajemnicy.

7. Prowadzone są wykazy osób i podmiotów, którym udostępniono lub powierzono przetwarzanie danych osobowych.

8. Dostęp osób nieposiadających stosownych upoważnień do pomieszczeń, w których przetwarzane są dane osobowe odbywa się wyłącznie za zgodą ADO lub w obecności i pod nadzorem osób upoważnionych.

9. Wykonane kopie zapasowe zbiorów danych osobowych przechowywane są w pomieszczeniu innym niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

§ 25. 1. Wszyscy pracownicy posiadający dostęp do danych osobowych przed przystąpieniem do pracy uczestniczą w szkoleniu dotyczącym obowiązujących przepisów prawa z zakresu ochrony danych osobowych oraz obowiązujących w Urzędzie procedur wewnętrznych. Każdy pracownik jest zobowiązany również do zapoznania się z niniejszą Polityką przed przystąpieniem do pracy.

2. Każdy z pracowników zobowiązany jest do zapoznania się z opublikowanym szkoleniem i jego aktualizacjami, znajdującym się w intranecie Urzędu w terminie 14 dni od jego umieszczenia.

3. Zakres czynności dla osoby upoważnionej do przetwarzania danych osobowych określa zakres odpowiedzialności tej osoby za ochronę przetwarzanych danych osobowych w stopniu adekwatnym do jej zadań na stanowisku pracy.

§ 26. 1. Nadzór nad dostępem do pomieszczeń, w których przetwarzane są dane osobowe sprawuje IOD lub wyznaczona przez niego osoba.

2. Pracownicy Urzędu są zobowiązani do informowania IOD o zauważonych próbach nieuprawnionego dostępu do pomieszczeń, o których mowa w ust. 1.

§ 27. 1. ADO w porozumieniu z IOD oraz ASI może określić pomieszczenia, do których dostęp osób sprzątających będzie ograniczony i możliwy tylko pod nadzorem osób uprawnionych do przebywania w tych pomieszczeniach.

2. Osoby opuszczające puste pomieszczenie, w którym przetwarzane są dane osobowe, zobowiązane są do zamknięcia drzwi na klucz. Zabrania się pozostawiania klucza w drzwiach po ich zewnętrznej stronie, za wyjątkiem sytuacji związanych z ochroną przeciwpożarową.

3. Zabrania się samowolnego dorabiania kluczy oraz ich wynoszenia poza siedzibę Urzędu. Każdorazowa potrzeba dorobienia dodatkowego klucza lub kluczy winna być zgłoszona IOD w celu rozpatrzenia zaistniałej potrzeby.

4. Po zakończeniu pracy pracownik zobowiązany jest wylogować się z systemu informatycznego, zamknąć okna w pomieszczeniu, umieścić materiały i dokumenty zawierające dane osobowe w szafach lub szufladach zamykanych na klucz, zgodnie z zasadą czystego biurka, czystej drukarki i czystej kopiarki (o ile takie urządzenia znajdują się w pomieszczeniu) zniszczyć w niszczarce wszystkie materiały zbędne w postaci błędnie utworzonej lub niepotrzebnej dokumentacji mającej krótkotrwałe znaczenie praktyczne, m.in. wydruków komputerowych i innych materiałów analogowych zawierających dane osobowe.

§ 28. 1. Udostępnianie drogą pocztową lub kurierską dokumentów i materiałów zawierających dane osobowe może odbywać się przesyłką rejestrowaną, a w przypadku danych zawartych na nośnikach magnetycznych, optycznych lub elektronicznych – przesyłką rejestrowaną za potwierdzeniem odbioru.

2. Pracownicy Urzędu przygotowujący przesyłki, o których mowa w ust. 1, powinni dołożyć należytej staranności celem zabezpieczenia ich zawartości przed nieuprawnionym dostępem do ich zawartości osób trzecich.

3. W Urzędzie dopuszcza się stosowanie zabezpieczeń technicznych i organizacyjnych innych, niż wymienione w § 24-29.

§ 29. 1. Sprawdzenia zgodności przetwarzania danych osobowych z przepisami prawa oraz wewnętrznych regulacji obowiązujących w tym zakresie w Urzędzie dokonuje IOD we współpracy z ASI w zakresie sprawdzeń dotyczących przetwarzania danych osobowych w systemie informatycznym. Odbiorcą sprawdzeń jest ADO lub w określonych przypadkach PUODO.

2. W przypadku otrzymania informacji o naruszeniu bezpieczeństwa danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia, IOD przeprowadza niezwłocznie sprawdzenie doraźne.

3. Sprawdzeniu podlega system informatyczny, w którym przetwarzane są dane osobowe, zabezpieczenia fizyczne i organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami prawnymi.

4. IOD przygotowuje plan sprawdzeń na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan obejmuje co najmniej jedno sprawdzenie i jest przedstawiany ADO nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu nim objętego.

5. Zbiory danych oraz system informatyczny służący do przetwarzania lub zabezpieczania danych osobowych są obejmowane sprawdzeniem co najmniej raz na pięć lat.

6. Dokumentowanie przez IOD czynności w toku sprawdzenia polega na tworzeniu materiałów w postaci papierowej lub elektronicznej w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i opracowania sprawozdania.

7. Po zakończeniu sprawdzenia IOD przygotowuje sprawozdanie, zgodnie z wytycznymi określanymi w RODO, które zawiera opis ustalonego stanu faktycznego podlegającego ocenie oraz analizę w zakresie przestrzegania przepisów o ochronie danych osobowych w odniesieniu do ustalonego stanu faktycznego. W sprawozdaniu IOD stwierdza, czy naruszone zostały przepisy o ochronie danych osobowych, a jeżeli tak, to jakie są planowane lub podjęte działania przywracające stan zgodny z prawem. Sprawozdanie jest sporządzane w postaci elektronicznej albo w postaci papierowej.

8. IOD przekazuje sprawozdanie ze sprawdzenia planowego do ADO nie później niż w terminie 30 dni od zakończenia sprawdzenia. Sprawozdanie ze sprawdzenia doraźnego przekazywane jest niezwłocznie po zakończeniu sprawdzenia.

§ 30. 1. Za zapewnienie pracownikom warunków organizacyjnych mających na celu zapewnienie należytego bezpieczeństwa danych osobowych odpowiada Gmina Dragacz reprezentowana przez Wójta Gminy w porozumieniu z osobami odpowiedzialnymi za poszczególne obszary działalności Gminy.

2. IOD w porozumieniu z ASI oraz osobami odpowiedzialnymi za poszczególne obszary działalności Gminy zapewnia bieżącą edukację pracowników dotyczącą zasad bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym i systemie tradycyjnym oraz wnioskuje do ADO o szkolenia w tym zakresie.

3. Na pracownikach oraz osobach upoważnionych do przetwarzania danych osobowych, w zakresie ich uprawnień i odpowiedzialności, ciąży obowiązek dbałości o zabezpieczanie danych osobowych przed ich udostępnieniem, zabraniem, przetwarzaniem z naruszeniem przepisów prawa przez osoby nieuprawnione oraz zmianą, uszkodzeniem, utratą lub zniszczeniem.

§ 31. 1. Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością wynikającą z obowiązujących przepisów prawa.

2. Odpowiedzialności podlega każdy pracownik, który:

1) przetwarza w zbiorze danych dane osobowe, do których nie jest upoważniony;

2) przetwarza w zbiorze danych dane, których przetwarzanie jest zabronione;

3) przetwarza w zbiorze danych dane niezgodne z celem stworzenia tego lub innych zbiorów;

4) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym;

5) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach;

6) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw.

3. Złamanie zasad PBI stanowi incydent, o którym powinien być niezwłocznie powiadomiony IOD. O podjęciu działań naprawczych decyduje ADO na podstawie projektu działań opracowanego przez IOD. W przypadku wystąpienia incydentu związanego z przetwarzaniem danych osobowych w systemie informatycznym, projekt naprawczy opracowuje i przedstawia również ASI.

4. Łamanie zasad wynikających z niniejszej PBI może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych i może skutkować nałożeniem kary porządkowej na zasadach określonych w przepisach prawa pracy oraz procedurach wewnętrznych, w szczególności w przypadku osoby, która po stwierdzeniu naruszenia bezpieczeństwa danych osobowych lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie IOD.

5. Udokumentowane umyślne złamanie zasad określonych w PBI jest traktowane jako ciężkie naruszenie obowiązków pracowniczych uzasadniające rozwiązanie stosunku pracy bez wypowiedzenia z winy pracownika

Rozdział 4.
Ogólne warunki korzystania z systemu informatycznego

§ 32. 1. Zasady zachowania bezpieczeństwa w systemie informatycznym obejmują wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę informacji przed ich nieuprawnionym przetwarzaniem.

2. Każdy Użytkownik systemu informatycznego stosowanego w Urzędzie do przetwarzania danych osobowych jest zobowiązany do zapoznania się z zasadami korzystania z tego systemu.

3. Korzystanie z funkcjonalności systemu informatycznego jest możliwe pod warunkiem nadania przez ASI uprawnień Użytkownika systemu informatycznego.

4. Szczegółowe procedury nadawania uprawnień do systemu informatycznego określa IZSI służącym do przetwarzania danych osobowych w Urzędzie.

§ 33. 1. Zgodnie z postanowieniami niniejszej PBI, zabrania się Użytkownikowi systemu informatycznego podejmowania jakichkolwiek czynności mających na celu naruszenie bezpieczeństwa przetwarzanych danych, w tym prób przełamania zabezpieczeń tego systemu.

2. W celu zapobieżenia nieautoryzowanemu dostępowi do systemu informatycznego Użytkownik nie może przechowywać danych służących do logowania do systemu w miejscach dostępnych dla innych osób oraz ujawniać danych służących do logowania innym osobom.

3. Zabronione jest korzystanie z systemu informatycznego z użyciem danych dostępowych innego Użytkownika.

4. Użytkownicy są zobowiązani do ustawienia ekranów monitorów w taki sposób, aby uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora.

5. Użytkownik zobowiązany jest do przestrzegania zasady „czystego biurka", w szczególności przed opuszczeniem swego stanowiska pracy powinien schować wszelkie dokumenty oraz informatyczne nośniki danych.

6. W czasie kopiowania, drukowania dokumentów zawierających dane osobowe, Użytkownik zobowiązany jest do zachowania zasady „czystej drukarki", „czystej kopiarki", w szczególności przed opuszczeniem stanowiska kopiowania/drukowania upewnić się, że w urządzeniach nie pozostały dokumenty zawierające dane osobowe.

7. Przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych z użyciem urządzeń mobilnych, Użytkownik jest zobowiązany do sprawdzenia, czy posiadane przez niego dane są należycie zabezpieczone przed dostępem osób nieupoważnionych.

8. Po zakończeniu przetwarzania danych osobowych, Użytkownik zobowiązany jest do należytego zabezpieczenia ich przed dostępem osób nieupoważnionych.

Rozdział 5.
Poczta elektroniczna

§ 34. 1. Użytkownik zobowiązany jest do dbania o bezpieczeństwo poczty elektronicznej, w szczególności do używania silnego hasła dostępu, nieotwierania załączników do poczty i linków pochodzących z nieznanych źródeł oraz zachowania ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej od znanych nadawców.

2. Szczegółowe procedury korzystania z poczty elektronicznej oraz konfiguracji sprzętu komputerowego Użytkownika systemu informatycznego reguluje IZSI służącym do przetwarzania danych osobowych w Urzędzie.

§ 35. W stosunku do pozostałych informacji podlegających ochronie, przetwarzanych w związku z działalnością Urzędu Gminy Dragacz, stosuje się zasady bezpieczeństwa określone w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2023 r. poz. 756 z późn. zm.);

Rozdział 7.
Postępowanie na wypadek zagrożenia bezpieczeństwa danych osobowych

§ 36. 1. Ryzyko w zakresie bezpieczeństwa informacji, w tym danych osobowych, definiuje się jako prawdopodobieństwo wystąpienia zagrożeń i powstanie szkód, zniszczeń oraz przerw lub zakłóceń prawidłowego funkcjonowania systemu tradycyjnego oraz systemu informatycznego, w których przetwarzane są dane osobowe.

2. Zarządzanie ryzykiem jest procesem identyfikacji zasobów, odpowiadających im podatności i zagrożeń, oceny prawdopodobieństwa ich wystąpienia, wielkości potencjalnych strat oraz przeciwdziałania i określenia kryteriów akceptowalności ryzyka.

3. Zarządzanie ryzykiem obejmuje możliwie jak najszybszą identyfikację ryzyka związanego z planowanym działaniem, ocenę stopnia wpływu ryzyka na uzyskane wyniki lub cele oraz zastosowanie odpowiednich środków kontroli ryzyka.

4. Proces zarządzania ryzykiem w zakresie bezpieczeństwa informacji, odnoszącym się do działalności Urzędu Gminy Dragacz, dokonywany jest przez IOD we współpracy z osobami odpowiedzialnymi za poszczególne obszary działalności (właścicielami ryzyka) oraz ASI w zakresie systemu informatycznego.

5. Pracownicy, do których przypisano poszczególne ryzyka (właściciele ryzyka), określają prawdopodobieństwo wystąpienia zidentyfikowanych ryzyk oraz ich skutek i wpływ na realizowane zadania z jednoczesnym wskazaniem istniejących mechanizmów kontroli i propozycją reakcji na ryzyko;

6. Wypełnione arkusze zarządzania ryzykiem przekazywane są do IOD. Na ich podstawie IOD, w przypadku ryzyk dotyczących bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym w porozumieniu z ASI, opracowuje roczne sprawozdania, które w postaci raportu o zidentyfikowanych ryzykach przekazuje ADO.

§ 37. 1. Niezależnie od corocznej oceny ryzyk, IOD przeprowadza ocenę ryzyk po każdorazowym wystąpieniu incydentu oraz każdorazowej zmianie mogącej wpływać na poziom ryzyka, w tym szczególnie zmianie struktury organizacyjnej, otoczenia dotyczącego realizacji umów z nowymi podmiotami, technologii, infrastruktury, pracowników, metod pracy, przepisów prawa.

2. Niezwłocznie po wystąpieniu incydentu, IOD przedstawia ADO wyniki oceny zidentyfikowanych ryzyk wraz z propozycjami działań korygujących i zapobiegawczych, do których należy w szczególności: określenie zadań do realizacji, zdefiniowanie odpowiedzialności, ram czasowych oraz propozycji zmian celem poprawy bezpieczeństwa informacji.

3. Na podstawie raportów i sprawozdań otrzymanych od IOD, ADO podejmuje ostateczną decyzję w zakresie realizacji działań zapewniających ochronę przetwarzanych informacji w szczególności:

1) zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2) utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
3) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
5) dokonanie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4
6) zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
   a) zagrożenia bezpieczeństwa informacji,
   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
7) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
   a) monitorowanie dostępu do informacji,
   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
8) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawieranie w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

12) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację systemu operacyjnego'

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,

d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

e) zapewnieniu bezpieczeństwa plików systemowych,

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i PBI;

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w sposób, umożliwiający szybkie podjęcie działań korygujących;

14) zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

§ 38. 1. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

1) próby naruszenia ochrony danych:

a) z zewnątrz - włamania do systemu, podsłuch, kradzież danych,

b) z wewnątrz - nieumyślna lub celowa modyfikacja danych, kradzież danych,

2) programy destrukcyjne: wirusy, konie trojańskie, makra, bomby logiczne;

3) awarie sprzętu lub uszkodzenie oprogramowania;

4) zabór sprzętu lub nośników z ważnymi danymi;

5) inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych;

6) usiłowanie zakłócenia działania systemu informatycznego.

2. Do typowych incydentów zagrażających bezpieczeństwu danych osobowych należą:

1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;

2) niewłaściwe zabezpieczenie sprzętu IT i oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;

3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek) w tym:

a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki ASI, użytkowników, utrata/zagubienie danych),

c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

3. Do typowych źródeł informacji o incydentach, zagrożeniach lub słabościach systemu zalicza się:

1) zgłoszenia od Użytkowników;

2) alarmy z systemów informatycznych;

3) analizy incydentów;

4) wyniki audytów / kontroli.

§ 39. Każdy pracownik, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować IOD lub ASI w sytuacjach dotyczących użytkowania systemu informatycznego. Zasady działania w takich przypadkach określa **tabela nr 1:**

Tabela nr 1. Zasady działania w przypadku zagrożenia lub naruszenia ochrony danych osobowych

G 1.	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej	Powiadomić IOD. Sporządzić raport.
G 2.	Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem Użytkownika.	Powiadomić IOD. Sporządzić raport.

§ 40. 1. W przypadku stwierdzenia wystąpienia zagrożenia, IOD prowadzi postępowanie wyjaśniające, w toku którego ustala zakres i przyczyny zagrożenia oraz jego potencjalne skutki, inicjuje ewentualne działania dyscyplinarne, rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości, dokumentuje prowadzone postępowania.

2. W przypadku stwierdzenia incydentu (naruszenia) IOD prowadzi postępowanie wyjaśniające, w toku którego.:

1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały i zabezpiecza ewentualne dowody oraz podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
2) ustala osoby odpowiedzialne za naruszenie;
3) inicjuje działania dyscyplinarne, wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;
4) dokumentuje prowadzone postępowania.

3. IOD jest odpowiedzialny za analizę incydentów naruszenia bezpieczeństwa, zagrożeń lub słabości systemu ochrony danych osobowych. Gdy stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa źródło powstania incydentu, zagrożenia lub słabości, zakres działań korygujących lub zapobiegawczych, termin realizacji oraz osobę odpowiedzialną.

4. IOD jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych. Po przeprowadzeniu działań korygujących lub zapobiegawczych, jest zobowiązany do oceny efektywności ich zastosowania i prowadzenia stosownej dokumentacji.

Rozdział 6.
Postanowienia końcowe

§ 41. 1. W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie obowiązujące przepisy prawa dotyczące ochrony danych osobowych.

2. Nad aktualnością PBI w Urzędzie czuwa IOD we współpracy z ASI w zakresie przetwarzania danych osobowych w systemie informatycznym.