ZARZĄDZENIE NR SO.0050.60.2018

Wójta Gminy Rogowo

z dnia 05 października 2018 r.

w sprawie: wprowadzenia zmian do Polityki Ochrony Danych Osobowych w Urzędzie Gminy w Rogowie.

Na podstawie art. 24 ust 1 i 2 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 oraz art. 33 ust.3 ustawy z dnia 8 marca 1990 o samorządzie gminnym (T. j. Dz. U. z 2018 r. poz. 994 ze zm.) zarządza się, co następuje:

§ 1

Wprowadza się zmiany w „Polityce Ochrony Danych Osobowych w Urzędzie Gminy w Rogowie", która stanowi załącznik nr1 do zarządzenia nr 28.2018 Wójta Gminy Rogowo z dnia 23 maja 2018 r. w sprawie wprowadzenie Polityki Ochrony Danych Osobowych w Urzędzie Gminy w Rogowie poprzez:

1. We "Wstępie" w ust. 3 dodaje się punkty k - p:

   "k) RODO - oznacza 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.Urz. UE L 119, s. 1).
   l) Dane wrażliwe - oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej,
   m) IODO lub Inspektor - oznacza Inspektora Ochrony Danych Osobowych,
   n) RCPD - oznacza Rejestr Czynności Przetwarzania Danych Osobowych,
   o) RKCP - oznacza Rejestr Kategorii Czynności Przetwarzania,
   p) RNOD - oznacza Rejestr Naruszeń Ochrony Danych,
   r) Ustawa – ustawa z dnia 10 maja 2018r. o ochronie danych osobowych."

2. W dziale II "Zgodność z prawem" dodaje się ust. 4 - 6:

   "4. Administrator spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a) Administrator weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.
   b) Administrator zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany w RODO i dokumentowane.
   c) Administrator stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.
   5. Administrator posiada zasady i metody zarządzania minimalizacją (privacy by default), a w tym:
   a) zasady zarządzania adekwatnością danych;
   b) zasady reglamentacji i zarządzania dostępem do danych;

c) zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności;

6. Privacy by design. Administrator zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów lub zadań Administrator uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu."

3. Dział IV otrzymuje nazwę "Analiza ryzyka" oraz otrzymuje brzmienie:

"1. Metodyka analizy ryzyka i zagrożeń przy przetwarzaniu danych osobowych precyzuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zagrożeń, która stanowi załącznik nr 4a - Metodyka analizy ryzyka i zagrożeń przy przetwarzaniu danych osobowych.

2. W przypadku konieczności przeprowadzenia oceny skutków dla ochrony danych, w celu zapewnienia najwyższego poziomu bezpieczeństwa, wymagane jest wykonanie co najmniej:

a) systematycznego opisu planowanych operacji przetwarzania i celów przetwarzania – zawarty w załączniku nr 1a – Rejestr zbiorów danych osobowych,
b) ocenę, czy operacje przetwarzane są niezbędne oraz proporcjonalne do celów zostało zawarte w załączniku nr 1a – Rejestr zbiorów danych osobowych,
c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą.
d) środki planowane w celu zapewnienia bezpieczeństwa."

4. W dziale V "Procedura postępowania z naruszeniami":

a) ust. 3 otrzymuje brzmienie:

"Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze na formularzu stanowiącym załącznik nr 5a – Rejestr Naruszeń."

b) ust. 5 i 6 otrzymują brzmienie:

"5. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je właściwemu organowi nadzorczemu chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

6. W przypadku naruszenia ochrony danych osobowych powodujących wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu."

c) dodaje się ust. 7 o treści:

"7. Zwolnienie z obowiązku zawiadomienia osoby o którym mowa w ust. 6 następuje jeśli:

a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności szyfrowanie,
b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby,
c) Wymagałoby ono niewspółmiernie dużego wysiłku."

5. W dziale VI "Instrukcja ochrony danych osobowych" ust. 2 otrzymuje brzmienie:

" Do stosowania zasad ochrony danych osobowych zobowiązani są wszyscy użytkownicy systemów tradycyjnych i informatycznych, a także wszyscy, którzy mogą mieć jakąkolwiek styczność z danymi osobowymi chociażby przypadkową. Użytkownicy i inne osoby składają odpowiednie oświadczenie, którego wzór stanowi załącznik nr 6b – Oświadczenie o poufności."

6. W dziale VII "Szkolenia" ust. 4 otrzymuje brzmienie:

" Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania, załącznik nr 6b – Oświadczenie o poufności."

7. Dział VIII otrzymuje nową nazwę "Rejestry" oraz treść:

"1. Administrator prowadzi rejestr czynności przetwarzania danych osobowych – załącznik nr 8a –Rejestr czynności przetwarzania danych osobowych.
2. RCPD stanowi formę dokumentowania czynności przetwarzania danych osobowych u Administratora. RCPD 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.
3. Administrator prowadzi RCPD, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
4. RCPD jest jednym z podstawowych narzędzi umożliwiających rozliczanie większości obowiązków ochrony danych.
5. Administrator prowadzi rejestr kategorii czynności przetwarzania - załącznik nr 8b - Rejestr kategorii czynności przetwarzania.
6. RKCP stanowi formę dokumentowania czynności przetwarzania danych osobowych u Administratora jako przetwarzającego w imieniu innego Administratora Danych. RKCP 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.
7. Administrator prowadzi RKCP, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
8. RKCP jest jednym z podstawowych narzędzi umożliwiających rozliczanie większości obowiązków ochrony danych."

8. Dodaje się Dział XII "Inspektor Ochrony Danych Osobowych" o treści:

"1. Status prawny i zadania Inspektora ochrony danych regulują przepisy Rozdziału IV Sekcji 4 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.
2. Inspektor ochrony danych w wykonywaniu swoich zadań podlega bezpośrednio Wójtowi Gminy Rogowo.
3. Do zadań Inspektora ochrony danych należy w szczególności:
a) informowanie Administratora oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach wynikających z rozporządzenia RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tych sprawach;
b) monitorowanie przestrzegania rozporządzenia RODO, innych przepisów dotyczących ochrony danych osobowych oraz prowadzenie szkoleń wewnętrznych zwiększających świadomość personelu DPS w zakresie zasad dotyczących ochrony danych,
c) pełnienie funkcji punktu kontaktowego dla właściwych organów i podmiotów zewnętrznych w kwestiach związanych z przetwarzaniem przez Administratora danych osobowych.

4. IODO nie rzadziej niż raz na kwartał przeprowadza audyt wewnętrzny stosowania dokumentacji ochrony danych osobowych oraz rozwiązań technicznych i organizacyjnych u Administratora.
5. Z audytu o którym mowa w ust. 4 IODO sporządza protokół, określający zakres kontroli, stan stosowania regulacji ochrony danych osobowych, a także zalecenia co do dalszego przetwarzania."

9. Dodaje się załącznik nr 8b - Rejestr kategorii czynności przetwarzania.

10. W załączniku nr 6a - Instrukcja Ochrony Danych Osobowych w Urzędzie Gminy w Rogowie:

a) W dziale 11 "Obowiązek zachowania poufności i ochrony danych osobowych" ust. 3 otrzymuje brzmienie:

" Osoby zapoznane z treścią niniejszej Instrukcji ODO lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności."

b) W dziale 13 "Postępowanie dyscyplinarne" ust. 2 ulega skreśleniu.

§ 2

Zobowiązuje się pracowników Urzędu Gminy w Rogowie do zapoznania się ze zmianami określonymi w niniejszym Zarządzeniu.

§ 3

Zarządzenie wchodzi w życie z dniem 05 października 2018 roku.

WÓJT

mgr Barbara Nowakowska

Załącznik Nr 4a do Zarządzenia
Nr SO.0050.60.2018
Wójta Gminy Rogowo
z dnia 05 października 2018 r.

METODYKA ANALIZY RYZYKA I ZAGROŻEŃ PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Urzędu Gminy

w Rogowie

Spis treści

Załączniki:

- załącznik nr 1 - Wzór tabeli szacowania ryzyka
- załącznik nr 2 - Wzór formularza analizy ryzyka

I. Podstawa prawna:

1. Niniejszy dokument zatytułowany „**Metodyka analizy ryzyka i zagrożeń przy przetwarzaniu danych osobowych**" (dalej jako **Analiza**) ma za zadanie określić zasady szacowania ryzyka i zagrożeń związanych z ochroną danych osobowych w Urzędzie Gminy w Rogowie (dalej jako **UG**).

   Niniejsza Analiza jest elementem kształtowania odpowiednich zabezpieczeń w zakresie ochrony danych osobowych.

2. Administrator Danych ze względu na ciążące na nim obowiązki wynikające z ustawy o ochronie danych osobowych oraz 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). (dalej jako **RODO**) zobowiązany jest do zastosowania środków technicznych i organizacyjnych, które mają zapewnić ochronę przetwarzanych danych osobowych, w świetle adekwatnych zagrożeń, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

3. Skuteczność zastosowanych środków powinna podlegać cyklicznym badaniom. Przy stosowaniu zabezpieczeń powinno się też uwzględniać zmieniające się warunki oraz postęp techniczny (informatyczny), co może powodować konieczność zmiany czy modernizowania wprowadzonych wcześniej przez Administratora Danych systemów ochrony. Analiza zagrożeń i ryzyka, określa środki zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
4. ADO jest zobowiązany dostosować środki bezpieczeństwa, zarówno techniczne, jak i fizyczne oraz organizacyjne, do wyników, jakie wykazała przeprowadzona analiza.

5. Przy sporządzaniu analizy ryzyka i zagrożeń ADO konsultuje się z IODO.

II. Podstawowe pojęcia i skróty:

1) **Analiza ryzyka** – systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka;
2) **Szacowanie ryzyka** – proces oceny i analizy ryzyka;
3) **Ocena ryzyka** – proces porównania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
4) **Postępowanie z ryzykiem** – wdrażanie środków modyfikujących ryzyko;
5) **Zarządzanie ryzykiem** – działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka;
6) **Ryzyko szczątkowe** – ryzyko pozostające po procesie postępowania z ryzykiem;
7) **Akceptowanie ryzyka** – decyzja, aby zaakceptować ryzyko;
8) **Bezpieczeństwo przetwarzania** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
9) **Zdarzenie związane z bezpieczeństwem przetwarzania** – zdarzenie związane z bezpieczeństwem przetwarzania, jako określonym stanem systemu, usługi lub czynności który wskazuje na możliwe naruszenie wewnętrznych polityk, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;
10) **Incydent związany z bezpieczeństwem przetwarzania** – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem przetwarzania, które stwarzają znaczne zakłócenia zadań i zagrażają bezpieczeństwu przetwarzania;
11) **Aktywa** – wszystko, co ma wartość dla organizacji, w tym również procesy przetwarzania;
12) **Czynnik zagrożenia** – to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;
13) **Dostępność** — należy przez to rozumieć właściwość określającą, że zasób jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy;

14) **Informatyczny nośnik danych** — należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;
15) **Integralność** — należy przez to rozumieć właściwość określającą, że zasób nie został zmodyfikowany w sposób nieuprawniony;
16) **Oprogramowanie złośliwe** — należy przez to rozumieć oprogramowanie, którego celem jest przeprowadzenie nieuprawnionych lub szkodliwych działań w systemie teleinformatycznym;
17) **Podatność** — należy przez to rozumieć słabość zasobu lub zabezpieczenia, która może zostać wykorzystana przez zagrożenie;
18) **Połączenie międzysystemowe** — należy przez to rozumieć techniczne albo organizacyjne połączenie dwóch lub więcej systemów teleinformatycznych, umożliwiające ich współpracę, a w szczególności wymianę danych;
19) **Poufność** — należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;
20) **Przekazywanie informacji** — należy przez to rozumieć zarówno transmisję informacji, jak i przekazywanie informacji na informatycznych nośnikach danych, na których zostały utrwalone bądź w każdy inny sposób transferujący dane;
21) **Zabezpieczenie** — należy przez to rozumieć środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko;
22) **Zagrożenie** — należy przez to rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach;
23) **RODO** - oznacza 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.Urz. UE L 119, s. 1).
24) **Dane** - oznaczają dane osobowe, wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, o ile co innego nie wynika wyraźnie z kontekstu.
25) **Dane wrażliwe** - oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub

orientacji seksualnej;

26) **IODO lub Inspektor** - oznacza Inspektora Ochrony Danych Osobowych

27) **Ustawa** – ustawa z dnia 10 maja 2018r. o ochronie danych osobowych;

28) **Przetwarzanie danych osobowych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

29) **Administrator Danych Osobowych (ADO)** – Wójt Gminy Rogowo;

III. Wymogi ogólne bezpieczeństwa przetwarzanych danych osobowych:

1. W czasie przetwarzania danych osobowych informacje mogą występować w postaci:
   a) plików lub informacji przechowywanych na dysku twardym komputera;
   b) plików lub informacji zapisanych na nośnikach komputerowych;
   c) wersji roboczych lub gotowych dokumentów na papierze.
2. Bezpieczeństwo przetwarzanych lub przechowywanych informacji zawierające dane osobowe wymaga:
   a) zapewnienia ochrony fizycznej stanowiska pracy i komputerowego przed nieuprawnionym dostępem;
   b) ochrony nośników technicznych i wydruków dokumentów wytwarzanych przy pomocy sprzętu komputerowego, w tym określenia zasad postępowania z nimi przed nieuprawnionym dostępem;
   c) zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujących się w zasobach systemu informatycznego;
   d) zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego dla upoważnionych użytkowników;
   e) zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywanych na nim czynności;
   f) zapewnienia możliwości kontroli nośników, na których przetwarzano lub

przechowywano dane osobowe,

g) zapewnienia możliwości kontroli dostępu do pomieszczeń w których przetwarzane są dane osobowe,

h) zapewnienia ochrony pomieszczeń w których są przechowywane dane osobowe,

i) zapewnienia odpowiednich rozwiązań organizacyjnych umożliwiających sprawną ochronę danych osobowych.

IV. Zasady określenia poziomu ryzyka:

1. Ocena ryzyka opiera się na wyliczeniu poziomu ryzyka ogólnego, na które składają się poszczególne ryzyka dla danych zdarzeń wpływających na ochronę danych osobowych.
2. Ryzyko ogólne wyliczane jest jako średnia arytmetyczna, w zaokrągleniu do pełnych liczb, wszystkich pojedynczych ryzyk dla poszczególnych zagrożeń procesu przetwarzania.
3. Ryzyko dla danego zagrożenia stanowi iloczyn prawdopodobieństwa wystąpienia ryzyka i skutków wywoływanych na aktywa.
4. Dla każdego procesu przetwarzania wykonuje się odrębne wyliczenie poziomu ryzyka.
5. Prawdopodobieństwo wystąpienia ryzyka określa się poprzez stosunek czynników pewności wystąpienia, ekspozycji oraz czasu wystąpienia.
6. Pewność wystąpienia ryzyka to określenie z jakim przypuszczeniem dane zagrożenie może wystąpić w przyszłości. Przy ocenie tego czynnika należy wziąć pod uwagę zdarzenia, które nastąpiły w przeszłości oraz informacje o zdarzeniach w podobnych profilach działalności.
7. Skala pewności wystąpienia zdarzenia powodującego ryzyko dla ochrony danych osobowych.

WARTOŚĆ	PEWNOŚĆ ZDARZENIA
< 0 >	Brak prawdopodobieństwa wystąpienia
< 1 – 3 >	Niskie prawdopodobieństwo wystąpienia
< 4 – 5 >	Zdarzenie losowe
< 6 – 7 >	Średnie prawdopodobieństwo wystąpienia
< 8 – 9 >	Wysokie prawdopodobieństwo
< 10 >	Pewne zdarzenie

8. Ekspozycja jest to czasookres wystawienia aktywa na działanie zdarzenia wywołującego ryzyko naruszenia ochrony danych osobowych.

9. Skala ekspozycji na zdarzenie powodujące ryzyko dla ochrony danych osobowych.

WARTOŚĆ	EKSPOZYCJA
< 0 >	Brak ekspozycji
< 1 – 3 >	Ekspozycja krócej niż 1h
< 4 – 5 >	Ekspozycja dłużej niż 1h, ale krócej niż 8h
< 6 – 7 >	Ekspozycja dłużej niż 8h, ale krótszy niż 24h
< 8 – 9 >	Ekspozycja dłużej niż 24h
< 10 >	Stała ekspozycja

10. Czas wystąpienia ryzyka to przypuszczalne określenie momentu w czasie potencjalnego wystąpienia zdarzenia wywołującego ryzyko dla ochrony danych osobowych.

11. Skala czasu wystąpienia zdarzenia powodującego ryzyko dla ochrony danych osobowych.

WARTOŚĆ	CZAS
< 0 >	Zdarzenie nieprzewidywalne w przyszłości
< 1 – 3 >	Zdarzenie wystąpi za dalej niż rok
< 4 – 5 >	Zdarzenie wystąpi w przeciągu roku
< 4 – 5 >	Zdarzenie wystąpi w przeciągu miesiąca
< 8 – 9 >	Zdarzenie wystąpi w przeciągu tygodnia
< 10 >	Zdarzenie wystąpiło lub trwa

12. Prawdopodobieństwo wystąpienia zagrożenia dla ochrony danych osobowych

wyliczane jest jako średnia arytmetyczna w zaokrągleniu do jednej dziesiątej.

13. W myśl RODO oraz Ustawy, każdy ADO powinien zapewnić takie warunki pracy, aby cechowały się one poufnością, integralnością i rozliczalnością, które stanowią podstawę do wyliczenia skutków dla zagrożenia dla aktywa ochrony danych osobowych.

14. Każde zauważone zagrożenie związane z poufnością, integralnością lub rozliczalnością, powinno być niezwłocznie zgłoszone ADO bądź wyznaczonemu IODO.

15. Poufność, to zapewnienie danym osobowym niemożności ich udostępniania nieupoważnionym osobom czy podmiotom.

16. Zapewnienie poufności wartości informacyjnych wynika z obowiązku wypełnienia nakładanych na ADO zadań, wynikających z ustaw, wraz z wszelkimi konsekwencjami organizacyjnymi i prawnymi.

17. Strategiczną częścią zabezpieczania danych w systemach informatycznych oraz w formie tradycyjnej przed utratą poufności jest odpowiednio prowadzony system szkoleń dla pracowników merytorycznych mających dostęp do informacji.

18. Utrata poufności informacji o zasadach funkcjonowania systemów i sieci oraz mechanizmach zabezpieczeń jest niezwykle ważna oraz wymaga położenia nacisku na przestrzeganie procedur przez osoby sprawujące opiekę nad systemami i siecią.

19. Skala identyfikacji skutków utraty zasobów dla atrybutu poufności danych osobowych.

WARTOŚĆ	SKUTKI
< 0 >	Brak skutków utraty poufności
< 1 – 3 >	Niski skutek utraty poufności
< 4 – 7 >	Średni skutek utraty poufności
< 8 – 9 >	Wysoki skutek utraty poufności
< 10 >	Całkowita utrata poufności

20. Integralność to zapewnienie, aby wszelkie modyfikacje wykonywane w systemie informatycznym oraz w formie tradycyjnej, w systemie jego katalogów oraz indywidualnych plikach posiadające w sobie dane osobowe były skutkiem rozważnych i zaplanowanych działań osób przetwarzających dane.

21. Integralność, to cecha zapewniająca, że dane nie zostały zmodyfikowane lub zniszczone w sposób nieautoryzowany.

22. Integralność danych dotyczy przede wszystkim wartości informacyjnych

przetwarzanych w postaci elektronicznej. Dlatego tak ważne jest zachowanie integralności dla bezpieczeństwa systemu i sieci.

23. ADO powinien objąć procedurami weryfikacji i rozliczania pracowników sprawujących opiekę nad systemami i siecią oraz wprowadzić bieżącą, regularną detekcję prób ingerencji do systemu informatycznego oraz wszelkie próby naruszenia jego struktury, ponieważ skutkiem takich działań jest uszkodzenie bazy danych i w rezultacie naruszenie zapisów RODO.

24. Skala identyfikacji skutków utraty zasobów dla atrybutu integralności danych osobowych.

WARTOŚĆ	SKUTKI
< 0 >	Utrata integralności nie występuje
< 1 – 3 >	Niski skutek utraty integralności
< 4 – 7 >	Średni skutek utraty integralności
< 8 – 9 >	Wysoki skutek utraty integralności
< 10 >	Bezwzględny skutek utraty integralności

25. Rozliczalność to cecha zapewniająca działanie podmiotu przetwarzającego dane osobowe, która może być przypisana w sposób jednoznaczny tylko temu, jednemu podmiotowi.

26. Skala identyfikacji skutków utraty zasobów dla atrybutu rozliczalności danych osobowych.

WARTOŚĆ	SKUTKI
< 0 >	Utrata rozliczalności nie występuje
< 1 – 3 >	Niski skutek utraty rozliczalności
< 4 – 6 >	Średni skutek utraty rozliczalności
< 7 – 8 >	Wysoki skutek utraty rozliczalności
< 9 >	Ekstremalny skutek utraty rozliczalności
< 10 >	Absolutny skutek utraty rozliczalności

27. Skutek wystąpienia zagrożenia na aktywa ochrony danych osobowych wyliczany jest jako średnia arytmetyczna wartości utraty poufności, integralności i rozliczalności w

zaokrągleniu do jednej dziesiątej.

28. Wzór tabeli szacowania ryzyka stanowi załącznik nr 1 do niniejszego dokumentu.

V. Składniki analizy ryzyka:

1. Przy dokonaniu analizy należy sprecyzować aktyw, proces przetwarzania dla którego analiza jest dokonywana.

2. W analizie należy określić charakter, zakres, kontekst i cel przetwarzania w oparciu o Rejestr Czynności Przetwarzania Danych Osobowych.

3. Analiza zawiera określenie obszaru wymogów objętych analizą ryzyka z uwzględnieniem ograniczeń i modyfikacji w zakresie wymogów spoczywających na organach administracji publicznej pod kątem RODO (bezpieczeństwo danych osobowych lub pozostały obszar wymogów).

4. Analiza obejmuje określenie analizowanych operacji na danych osobowych, a także określenie wdrożonych zabezpieczeń (środków technicznych lub organizacyjnych służących eliminowaniu lub ograniczeniu wystąpienia zagrożeń).

5. Analiza zawiera zweryfikowanie czy dany rodzaj przetwarzania zawiera elementy wskazane w art. 35 ust. 3 oraz ust. 4 RODO.

6. ADO dokonuje identyfikacji podatności (luk w systemie ochrony danych osobowych) zarówno systemów informatycznych jak i rozwiązań organizacyjnych zabezpieczeń ochrony danych osobowych.

7. Analiza ryzyka opiera się na identyfikacji zagrożeń w ramach poszczególnych wymogów poprzez ich enumeratywne wyliczenie wraz ze wskazaniem prawdopodobieństwa wystąpienia i wskazaniem skutków dla ochrony danych osobowych wyliczone zgodnie z zapisami rozdziału IV.

8. Analiza zawiera wskazanie jakie prawa lub wolności osób fizycznych są zagrożone.

9. Obejmuje również wskazanie czy w związku z przeprowadzoną oceną ryzyka

zidentyfikowano, że dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

10. Jeśli zgodnie z ust. 9 odpowiedź na zadane pytanie wynosi tak, należy:

a) sporządzić systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
b) przeprowadzić ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
c) określić środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

11. Analiza zawiera wskazanie poziomu ryzyka wystąpienia każdego zagrożenia, a także ogólny poziom ryzyka dla systemu ochrony danych osobowych w kontekście analizowanego aktywa.

12. W analizie należy podjąć decyzję w odniesieniu do zidentyfikowanego ryzyka zgodnie z rozdziałem VI.

13. W analizie ADO określa podejmowane działania naprawcze, które następnie należy aktualizować i monitorować.

14. Wzór formularza analizy ryzyka stanowi załącznik numer 2 do niniejszego dokumentu.

VI. Poziom ryzyka i sposoby odpowiedzi na ryzyko:

1. Na podstawie oszacowanych ryzyk dla poszczególnych zagrożeń wyliczonych zgodnie z poprzedzającymi rozdziałami określa się poziomy ryzyka w skali od 0 do 100.

WARTOŚĆ	POZIOM RYZYKA
<1-20>	**NISKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<21-60>	**ŚREDNI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<61-80>	**WYSOKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<81-100>	**MAKSYMALNY** poziom ryzyka utraty bezpieczeństwa danych osobowych

2. Poziomy ryzyka utraty bezpieczeństwa danych osobowych:
   a) **NISKI** – niskie szkody w przypadku realizacji zagrożenia i niska możliwość jego wystąpienia;
   b) **ŚREDNI** – wysokie szkody w przypadku realizacji zagrożenia i niska możliwość jego realizacji bądź niskie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego realizacji;
   c) **WYSOKI** – wysokie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego wystąpienia;
   d) **MAKSYMALNY** – wysokie szkody w przypadku realizacji zagrożenia oraz wysoka możliwość jego wystąpienia, skutkująca nie tylko na organizację, ale na podmioty trzecie.

3. ADO po oszacowaniu ryzyka przystępuje do etapu postępowania z ryzykiem. Koniecznym jest podjęcie działania, które będzie odpowiedzią na oszacowany poziom występującego ryzyka. W ramach postępowania z ryzykiem możemy podjąć cztery różne działania:
   a) unikanie ryzyka - odejście od działań, które wiążą się z ryzykiem, jeżeli ryzyko jest duże, a aktyw, w którym ono występuje nie przynosi odpowiednich korzyści,
   b) ograniczanie ryzyka (redukcja) - podjęcie działań ograniczających ryzyko lub zmniejszających podatność,
   c) przekazanie ryzyka - przeniesienie ryzyka na podmiot zewnętrzny, wtedy odpowiedzialność przekazujemy w odpowiednich zapisach umowy,
d) akceptacja ryzyka - aprobata ryzyka kiedy koszty działań w celu niwelowania ryzyka przekraczają oczekiwane korzyści, bądź występują określone trudności w przeciwdziałaniu ryzyka.

VII. Postanowienia końcowe:

1. W sprawach nieobjętych niniejszym dokumentem mają zastosowanie odpowiednie przepisy prawa w szczególności 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) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000)
2. Każda osoba upoważniona do dokonania analizy ryzyka w UG jest obowiązana do zapoznania się oraz stosowania postanowień niniejszego dokumentu.

Załącznik nr 1 do Metodyki analizy ryzyka i zagrożeń przy przetwarzaniu danych osobowych

Tabela szacowania ryzyka

Przedmiot analizy:

Zakres i charakter analizy:

L.P.	Zagrożenie	Prawdopodobieństwo			Skutki dla ochrony danych osobowych			Wskaźnik prawdopodobieństwa	Wskaźnik skutku na aktywa	Ryzyko
		Pewność wystąpienia	Ekspozycja	Czas	Poufność	Integralność	Rozliczalność			
1										
2										0
3										0
4										0
5										0
6										0
7										0
8										0
9										0
10										0
11										0
12										0
13										0
14										0
15										0
16										0
17										0
18										0
19										0
20										0

Formularz analizy ryzyka

Dane wejściowe

Przedmiot analizy	
Punkty odniesienia analizy (charakter, zakres, kontekst i cele przetwarzania)	
Czy oceniany rodzaj przetwarzania polega na: a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną; b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 rodo, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 rodo; c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie; lub d) podlega art. 35 ust. 4 rodo.	
Oceniane operacje na danych osobowych	
Obszar wymogów	

Dane wyjściowe

Zidentyfikowane podatności	
Wdrożone (stosowane) zabezpieczenia	
Zidentyfikowane zagrożenia	
Ryzyko (naruszenia praw lub wolności osoby fizycznej)	
Poziom ryzyka ogólnego	
Czy w związku z przeprowadzoną oceną ryzyka zidentyfikowano, że dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych?	

Działania naprawcze	

Zał. Nr 6. do RODO

Rejestr Naruszeń Ochrony Danych w urzędzie Gminy Rogowo

Lp.																			

Rejestr kategorii czynności przetwarzania

Nazwa i dane kontaktowe przetwarzającego	
Nazwa	
Adres	
Email	
Telefon	

Inspektor Ochrony Danych (jeśli powołano)	
Nazwa	
Adres	
Email	
Telefon	

Przedstawiciel (jeśli wyznaczono)	
Nazwa	
Adres	
Email	
Telefon	

6b- Oświadczenie Poufności

OŚWIADCZENIE	
Imię i nazwisko	
Stanowisko służbowe	
Nazwa referatu	

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności ogólnego Rozporządzenia o ochronie danych UE 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) (Dz.Urz. UE L 119, s. 1) oraz Ustawy o Ochronie Danych Osobowych oraz odnośnymi wymaganiami "Polityki Ochrony Danych Osobowych".

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach
- zachowania w tajemnicy danych osobowych do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Ustawy o Ochronie Danych Osobowych oraz Rozporządzenia o ochronie danych UE 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) (Dz.Urz. UE L 119, s. 1).

.....
(imię, nazwisko i podpis osoby przyjmującej oświadczenie)

.....
(data i podpis składającego oświadczenie)