ANALIZA RYZYKA

RODO

zgodnie z art. 5 ust. 2 oraz Motywem 76 Preambuły 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).

Rozdzielnik:	Dokument do użytku wewnętrznego
Podmiot:	Urząd Gminy Augustów
z dnia:	20.12.2018
Zatwierdził(a):	…… podpis administratora danych

1. DEFINICJE

Administrator Danych – jest to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

Aktywa - kontrolowane przez jednostkę zasoby majątkowe o wiarygodnie określonej wartości, uzyskane w wyniku przeszłych zdarzeń, które spowodują w przyszłości wpływ do jednostki korzyści ekonomicznych;

Identyfikowanie ryzyka – szereg czynności polegających na określeniu sytuacji, które mogą się wydarzyć i spowodować straty/naruszenie;

Kontekst – informacje wiążące się z działaniem jednostki, m.in. informacje dotyczące środowiska prawnego, społecznego, politycznego, finansowego czy też technologicznego, np. przepisy dotyczące ochrony danych osobowych;

Akceptacja ryzyka – określenie dopuszczalności danego ryzyka, definiowane poprzez wartość progową, przy przedziałach ryzyka;

Naruszenie ochrony danych osobowych - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

Ocena ryzyka – czynność polegająca na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie ustanawiania kontekstu działania podmiotu;

RODO - Rozporządzenie 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);

Szacowanie ryzyka – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka;

Zabezpieczenie - środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia.

2. WSTĘP

Każdy podmiot, jednostka, bądź organizacja przetwarzająca dane narażona jest na wpływ czynników wewnętrznych oraz zewnętrznych, które mogą spowodować naruszenie bezpieczeństwa, prowadzące do przypadkowego lub niezgodnego z prawem: zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia, bądź dostępu do danych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Zgodnie z art. 24 ust. 1 jednym z zadań Administratora Danych jest wdrożenie odpowiednich zabezpieczeń, aby przetwarzanie danych odbywało się w zgodzie z RODO. Z pomocą przychodzą dokumenty: Analiza ryzyka RODO, a następnie Ocena skutków ryzyka dla ochrony danych osobowych, które są częścią ciągłego procesu udoskonalania systemu zarządzania bezpieczeństwem informacji. W celu przygotowania i przeprowadzenia analizy, wymagane jest profesjonalne podejście do zakresu ochrony informacji oraz danych, które pozwoli poznać szczegóły przeprowadzanych operacji przetwarzania danych wraz z warunkami środowiska, w którym odbywa się przetwarzanie. "Analiza ryzyka RODO", która będzie także punktem wyjścia do Oceny skutków ryzyka, pozwoli na zwiększenie poziomu bezpieczeństwa przetwarzanych danych osobowych.

Zapisy RODO uprawniają Administratora Danych do przetwarzania danych, gdy:

- upoważnia go do tego:
  - podstawa prawna;
  - wyrażenie zgody osoby, której dane dotyczą;
  - przetwarzanie jest niezbędne do wykonania umowy;
  - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
  - przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
  - przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
  - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.
- przy przetwarzaniu danych zapewniona jest im poufność, integralność oraz dostępność;
- dane osobowe zostaną adekwatnie zabezpieczone za pomocą wdrożonych środków technicznych jak i organizacyjnych gwarantujących odpowiedni poziom bezpieczeństwa, pamiętając, że im wyższe ryzyko naruszenia występuje, tym wyższy poziom ochrony należy zastosować. Zwracając uwagę na szybki postęp technologiczny oraz podnoszenie standardów bezpieczeństwa, stosowane rozwiązania powinny pomóc na bieżąco mierzyć i oceniać ich adekwatność oraz aktualność.

Decydując o doborze środków technicznych i organizacyjnych, należy uwzględnić poniższe czynniki:

- stan wiedzy technicznej;
- koszt wdrożenia wymaganych zabezpieczeń;
- charakter, zakres, kontekst i cel przetwarzania;
- ryzyko naruszenia praw i wolności osób fizycznych.

RODO, ze względu na szereg ogólnych zapisów wskazuje na możliwość:

- tworzenia kodeksów podstępowania, których zakres doprecyzuje zastosowanie dokumentu;
- przeprowadzenia mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych, które świadczą o spełnieniu obowiązków nałożonych na Administratorów.

Środkiem organizacyjnym pomagającym zapewnić bezpieczeństwo jest wydane stosowne upoważnienie każdej osobie przetwarzającej dane osobowe i zatrudnionej u Administratora. Nie należy zapominać, o zaznajomieniu pracowników z zasadami ochrony danych osobowych zastosowanych w podmiocie oraz pouczeniu o zobowiązaniu do zachowania tajemnicy, w związku z przetwarzanymi danymi.

3. OPIS PROCEDURY ZARZĄDZANIA RYZYKIEM

Przepis art. 5 ust. 1 RODO wprowadza osiem zasad przetwarzania danych osobowych, zawartych w sześciu punktach:

- zasadę legalności, rzetelności i przejrzystości przetwarzania (zgodności z prawem);
- zasadę celowości (ograniczenia celu);
- zasadę minimalizacji danych (adekwatności, proporcjonalności);
- zasadę prawidłowości (poprawności);
- zasadę ograniczenia czasowego (czasowości);
- zasadę odpowiedniego bezpieczeństwa (integralności i poufności danych).

Najważniejszą z powyższych zasad jest zasada legalności, której przestrzeganie Administrator Danych musi być w stanie wykazać. Zasada legalności oznacza wymóg, aby dane osobowe były przetwarzane zgodnie z prawem, a więc przede wszystkim zgodnie z RODO. Obowiązek legalności przetwarzania danych to przede wszystkim konieczność spełnienia przesłanki uprawniającej do takiego przetwarzania. Przesłanki, w zależności od kategorii danych, zostały określone w art. 6 i 9 RODO. Ponadto legalność oznacza zgodność z pozostałymi

przepisami RODO oraz obowiązującymi ustawami i wydanymi na ich podstawie aktami wykonawczymi.

Bezpieczeństwo danych osobowych powinno być odpowiednie. Z analizy motywów i artykułów RODO dowiemy się, że bezpieczeństwo danych ma być odpowiednie do ryzyka naruszenia praw i wolności osób, których dane dotyczą. Oznacza to, że poziom bezpieczeństwa powinien być dostosowany do tego, jaką szkodę lub krzywdę może wyrządzić osobom naruszenie bezpieczeństwa ich danych. Realizacja zasady odpowiedniego bezpieczeństwa będzie więc miała ścisły związek z szacowaniem ryzyka przetwarzanych danych. W zależności od rodzaju posiadanych danych, sposobu ich przetwarzania czy wielkości podmiotu będącego administratorem danych konieczne jest zastosowanie odpowiednich środków bezpieczeństwa minimalizujących ryzyko utraty kontroli nad przetwarzanymi danymi.

Zagadnienie dotyczące zasady odpowiedniości bezpieczeństwa w połączeniu z zasadą rozliczalności polega na tym, że jeśli nie zostanie przeprowadzona analiza i klasyfikacja ryzyka naruszenia ochrony danych, a w jej ramach ryzyka i konsekwencji naruszenia praw i wolności osób, nie będzie można wykazać, że zastosowane zostały odpowiednie środki bezpieczeństwa. Należy więc ocenić ryzyko, żeby zastosować odpowiednie do niego środki. Administrator danych powinien położyć nacisk na kwestie bezpieczeństwa, uwzględniając zagrożenia pochodzące zarówno z zewnątrz, jak i wewnątrz podmiotu. Kluczowa będzie analiza oraz podnoszenie poziomu zabezpieczeń. Digitalizacja zasobów i powszechne wykorzystywanie nowoczesnych technologii sprawiają, że sprawna realizacja celów biznesowych zależna jest od bezpieczeństwa zasobów informacyjnych i usług oraz infrastruktury teleinformatycznej umożliwiającej korzystanie z cyberprzestrzeni. Zastosowanie przez administratora danych systemów zapobiegających wyciekom danych, których ujawnienie może narazić podmiot na odpowiedzialność karną, cywilną lub innego rodzaju straty jest konieczne w aspekcie ochrony danych oraz informacji. Zasada bezpieczeństwa musi być zgodna z zasadą legalności i minimalizacji.

Niezależnie od wprowadzonej w art. 5 ust. 2 RODO zasady rozliczalności, zgodnie z którą administrator jest odpowiedzialny za przestrzeganie zasad przetwarzania, w tym zasady legalności, musi być w stanie wykazać ich przestrzeganie. Dodatkowo w art. 7 ust. 1 RODO podkreślono, że jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Administrator musi zatem pamiętać o utrwaleniu faktu uzyskania zgody na przetwarzanie danych w celu wykazania, w szczególności przed organem nadzorczym, że otrzymał zgodę na przetwarzanie danych osobowych. Zgoda osoby, której dane dotyczą, musi mieć charakter uprzedni w stosunku do przetwarzania jej danych przez administratora.

Zarządzanie ryzykiem opiera się na wdrożeniu schematu postępowania nazwanego cyklem Deminga. Jest to proces polegający na ciągłej poprawie danego zagadnienia, by osiągnąć jak najwyższy poziom realizacji. Cykl Deminga charakteryzuje się czterema etapami:

- zaplanuj;
- wykonaj;
- sprawdź;
- popraw.

Jeśli po wykonaniu ostatniego etapu nadal nie udało się osiągnąć wyznaczonego poziomu realizacji, należy całą procedurę ponowić. Dopiero w przypadku odniesienia oczekiwanych rezultatów, można uznać całą procedurę jako normę (standard) i jedynie monitorować prawidłowość jej działania.

Dla zagadnienia ochrony danych osobowych przyjęto poniższy schemat, gdzie zastosowano odpowiednie pojęcia niezbędne przy Analizie Ryzyka RODO.

- Kontekst – wyznaczenie zagrożonych elementów podmiotu, które mają pośredni i bezpośredni wpływ na ochronę danych osobowych;
- Szacowanie ryzyka – określenie występujących w podmiocie zagrożeń, skutków ich wystąpienia oraz prawdopodobieństwa, czy dane zagrożenie może nastąpić;
- Postępowanie z ryzykiem – wybór jednej ze ścieżek postępowania (rysunek poniżej);
- Sprawdzenie – zweryfikowanie, czy po zmianach dla danego kontekstu występuje jeszcze zagrożenie przy przetwarzaniu danych osobowych.

4. OPIS METODY SZACOWANIA RYZYKA – SKALA PIĘCIOSTOPNIOWA

Do sporządzenia Analizy ryzyka RODO, obejmującej wszystkie możliwe zagrożenia oraz konteksty przetwarzań danych osobowych, posłużyła metoda szacowania ryzyka na podstawie skali pięciostopniowej. W tej metodzie korzysta się z dwóch następujących parametrów ryzyka: skutków wystąpienia danego zagrożenia oraz prawdopodobieństwa z jakim zagrożenie może wystąpić. Szacowanie zarówno skutków jak i prawdopodobieństwa określa na pięciu poziomach (w skali od 1 do 5): bardzo małym, małym, średnim, dużym i bardzo dużym dla każdego występującego zagrożenia, zgodnie z tabelą przedstawioną poniżej:

Poziom skutku i prawdopodobieństwa	Wartość skutku i prawdopodobieństwa
Bardzo małe	1
Małe	2
Średnie	3
Duże	4
Bardzo duże	5

Tym sposobem szacuje się parametry wszystkich poziomów skutków oraz prawdopodobieństw, które mogą wystąpić dla danego zagrożenia. Następnie zgodnie z tabelą zaprezentowaną poniżej należy określić poziomy danego ryzyka – w skali od 1 do 25, korzystając ze wzoru: R = s * p, gdzie:

R – ryzyko dla danego zagrożenia;

s – poziom skutku zagrożenia;

p – poziom prawdopodobieństwa wystąpienia zagrożenia.

	Prawdopodobieństwo wystąpienia zagrożenia				
Skutek wystąpienia zagrożenia	**Bardzo małe**	**Małe**	**Średnie**	**Duże**	**Bardzo duże**
Bardzo małe	Bardzo małe	Bardzo małe	Małe	Małe	Małe
Małe	Bardzo małe	Małe	Małe	Małe	Średnie
Średnie	Małe	Małe	Średnie	Średnie	Średnie
Duże	Małe	Małe	Średnie	Duże	Duże
Bardzo duże	Małe	Średnie	Średnie	Duże	Bardzo duże

Oszacowaną wartość ryzyka danego zagrożenia przyporządkowuje się odpowiedniemu poziomowi ryzyka według tabeli:

Poziom ryzyka	Wartość ryzyka
Bardzo małe	1-2
Małe	3-8
Średnie	9-15
Duże	16-20
Bardzo duże	21-25

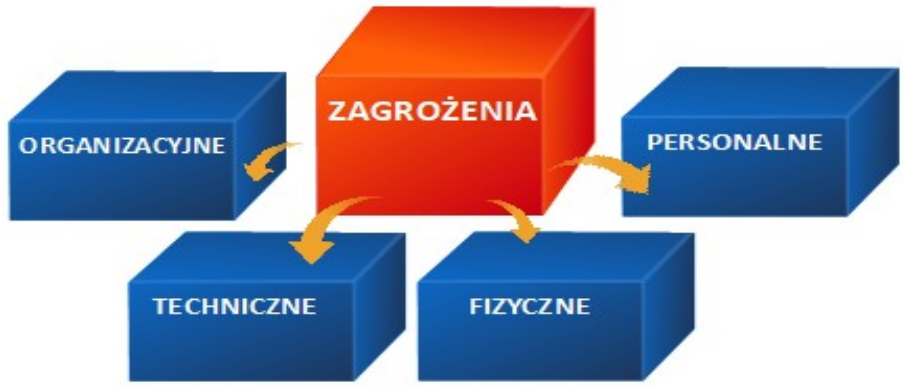
Powyższa metoda pozwala oszacować ryzyko dla każdego zagrożenia, uwzględniając poziom skutków i prawdopodobieństwa, dając tym samym możliwość określenia, czy dane ryzyko jest akceptowalne.

Poziom ryzyka	
Bardzo małe	Akceptowalne
Małe	Akceptowalne
Średnie	Akceptowalne
Duże	Akceptowalne
Bardzo duże	**Nieakceptowalne**

5. KONTEKST I ZAGROŻENIA

Ustalenie kontekstu jest podstawą do prawidłowego sporządzenie Analizy ryzka RODO, która jest punktem wyjścia do Oceny skutków ryzyka dla ochrony danych. Na wstępie należy przede wszytkim określić możliwe zagrożenia, które mogą mieć negatywny wpływ na uwarunkowania związane z działaniem podmiotu, a w szczególności dotyczące posiadanych danych osobowych w wersji papierowej, sprzętu, oprogramowania, pomieszczeń oraz nośników danych.

Na wymienione powyżej aktywa wpływają różne czynniki zagrożeń, zarówno zewnętrzne, jak i wewnętrzne, dlatego ważne jest sporządzenie ich listy. Identyfikacja zasobów i zagrożeń powinna być przeprowadzona na odpowiednim poziomie szczegółowości, co zapewni prawidłowe oszacowanie poszczególnych ryzyk i poziomów akceptacji. Zagrożenia można podzielić na kilka grup:



Najczęściej występujące zagrożenia, prowadzące do naruszeń:

a) Organizacyjne:

- brak nadanych upoważnień osobom przetwarzającym dane osobowe;
- brak wdrożonych polityk i procedur dotyczących ochrony danych osobowych;
- brak powołania Inspektora Ochrony Danych Osobowych w sytuacji, gdy wyznaczenie jest obligatoryjne;
- nieuprawniony dostęp do pomieszczenia, w którym są przetwarzanie dane osobowe.

b) Techniczne:

- atak hakerski;
- działanie złośliwego oprogramowania (wirusy);
- awaria nośników danych;
- awaria sprzętu sieciowego;
- awaria serwerów;
- awaria zasilania – brak UPS;
- celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych;
- przesłanie danych drogą mailową do złego odbiorcy.

c) Fizyczne:

- zalanie/powódź;
- pożar;
- kradzież sprzętu z danymi;
- kradzież danych w wersji papierowej;

- zniszczenie danych osobowych bez użycia niszczarki;
- atak terrorystyczny;
- zwarcie instalacji;
- nieodpowiednie przechowywanie danych;
- utrata przetwarzanych danych;
- niewystarczający poziom zabezpieczeń pomieszczeń.

d) Personalne:

- nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik;
- wejście w posiadanie danych osobowych przez osobę nieuprawnioną;
- udostępnianie danych osobowych osobom nieupoważnionym;
- udostępnianie haseł innym pracownikom;
- nie zachowanie tajemnicy służbowej dotyczącej danych osobowych przez pracowników podczas pracy, jak i po jej zakończeniu;
- otwieranie podejrzanych maili, mogących zawierać wirusy komputerowe;
- nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym.

6. TABELA SZACOWANIA RYZYKA

Lp.	Zagrożenie	Aktywa zagrożone	Skutki	Prawdopodobieństwo	Ryzyko	Akceptacja ryzyka
1	Zalanie/powódź	SP, P, OP, N, WP	2	1	3	Akceptowalne
2	Pożar	SP, P, OP, N, WP	4	4	16	Akceptowalne
3	Kradzież danych w wersji papierowej	WP	3	3	9	Akceptowalne
4	Kradzież sprzętu z danymi	SP, OP	5	3	15	Akceptowalne
5	Atak hakerski	SP, OP, N	4	3	12	Akceptowalne
6	Awaria nośników danych	N	4	5	20	Akceptowalne
7	Utrata danych (brak kopii zapasowych)	OP	4	5	20	Akceptowalne
8	Awaria sprzętu sieciowego	SP, OP	4	3	12	Akceptowalne
9	Awaria serwerów	OP	4	3	12	Akceptowalne
10	Nieuprawnione przeniesienie informacji	OP	3	2	6	Akceptowalne

	zawierających dane osobowe na inny nośnik					
11	Wejście w posiadanie danych osobowych przez osobę nieuprawnioną	OP, N, WP	4	3	12	Akceptowalne
12	Udostępnianie danych osobowych osobom nieupoważnionym	OP, N, WP	5	3	15	Akceptowalne
Aktywa: SP- Sprzęt, P – Pomieszczenia, OP – Oprogramowanie, N – Nośniki danych, WP – Dane w wersji papierowej.						

7. WNIOSKI

W podmiocie Urząd Gminy Augustów po przeprowadzeniu analizy dotyczącej ryzyka wystąpienia naruszeń w zakresie ochrony danych osobowych, zwanej Analizą Ryzyka RODO, zwrócono uwagę, iż Administrator Danych dołożył wszelkich starań, by poziom ochrony danych osobowych był jak najwyższy. Wszystkie występujące zagrożenia cechują się akceptowalnym poziomem ryzyka, dzięki czemu nie będą miały wpływu na naruszenia dotyczące ochrony danych osobowych. Jednakże Administrator Danych powinien sukcesywnie kontrolować, czy stopień ryzyka pojawienia się naruszenia nie zwiększy się w przyszłości.

W przypadku wystąpienia zbyt dużego ryzyka cząstkowego (dotyczącego jednego zagrożenia) należy dołożyć wszelkich starań, by to ryzyko zminimalizować. Artykuł 32 ust. 1 RODO wskazuje działania i środki, które mogą być wdrożone do minimalizacji ryzyka:

- pseudonimizacja i szyfrowanie danych osobowych,
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Należy jednak pamiętać, że są to przykłady możliwych działań - konkretne rozwiązania zależą od Administratora Danych i są wynikiem Analizy Ryzyka RODO. RODO wskazuje również przypadki, gdy wywiązywanie się z obowiązku przeprowadzenia analizy ryzyka będzie ograniczone. Ma to miejsce w sytuacji, gdy organizacja stosuje zatwierdzony przez organ nadzorczy kodeks postępowania lub mechanizm certyfikacji. Należy zwrócić uwagę, że konieczne jest, aby takie dokumenty uzyskały formalną akceptację UODO (Urząd Ochrony Danych Osobowych), ponieważ bez takiej akceptacji nie dają ochrony przewidzianej przepisami.

.....
(data i podpis Administratora Danych)