WÓJT GMINY
42-283 BORONÓW
ul. Dolna 2
Tel. 34 366 98 15, fax 34 366 98 14

ZARZĄDZENIE Nr 179/ 2018
Wójta Gminy Boronów
z dnia 05.12. 2018 r.

w sprawie przyjęcia zasad przeprowadzania analizy ryzyka w obszarze ochrony danych osobowych w Urzędzie Gminy Boronów

Na podstawie art. 32 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) (Dz.U.UE.L.2016.119.1) zarządzam, co następuje:

§ 1

Wprowadza się zasady przeprowadzenia analizy ryzyka w obszarze ochrony danych osobowych, w postaci załącznika nr 1 do niniejszego zarządzenia

§ 2

Analizę ryzyka przeprowadza się w oparciu o metodę przyjętą w załączniku nr 2 do niniejszego zarządzenia.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania

WÓJT
Krzysztof Bełkot

Załącznik nr 1 do Zarządzenie Nr 179/2018
z dnia 05.12.2018 r. w sprawie zasad
przeprowadzania analizy ryzyka w
obszarze ochrony danych osobowych

ZASADY PRZEPROWADZANIA ANALIZY RYZYKA

Celem zarządzania ryzykiem jest zapewnienie skutecznego przestrzegania przepisów prawa, skutecznej ochrony praw i wolności osób, których dane są przetwarzane oraz skutecznej ochrony Administratora.

Etapu zarządzania ryzykiem
Na proces zarządzania ryzykiem składa się z:

1. szacowanie ryzyka:
    a. identyfikacja zagrożeń
    b. ocena ryzyka
2. reakcja na ryzyko
3. monitorowanie ryzyka
4. działania korekcyjne

Szacowanie ryzyka
Szacowanie ryzyka – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka (definicja przyjęta zgodnie z normą PN-ISO/IEC 25005:2011)
Identyfikacja ryzyka ma na celu wskazanie niekorzystnych zjawisk, zdarzeń, praktyk, itp., które w konsekwencji mogą zagrozić realizacji celów i zadań oraz ochrony praw i wolności osób, których dane są przetwarzane. Zagrożenie wg PN-ISI Guide 73:2012 to źródło potencjalnej szkody. Zagrożenie może być uszczegółowione przez podanie pochodzenia (np. zagrożenie mechaniczne, zagrożenie elektryczne) albo charakteru potencjalnej szkody (np. ujawnienie poufnych danych).

Ocena ryzyka
Zidentyfikowane ryzyka poddawane są ocenie mającej na celu określenie prawdopodobieństwa wystąpienia ryzyka oraz jego wpływu.
Oceny ryzyka dokonywana jest różnymi metodami, w tym:

- metodą ilościową - bazującą na informacjach i danych z przeszłości, które mają charakter liczbowy: ilość, częstotliwość, zmienność,
- metodą jakościową - stosowaną jeśli ryzyko nie poddaje się obliczeniom lub brak jest dostępu do danych je charakteryzujących, albo gdy ich uzyskanie byłoby zbyt kosztowne;

jakość oceny jest tu częściowo oparta na kompetencjach (wiedzy, doświadczeniu) osób dokonujących tych analiz, a częściowo ma charakter intuicyjny, tzw. profesjonalny osąd,

- metodą ilościowo-jakościową - będącą połączeniem wskazanych wyżej dwóch technik.

Określenie wpływu

polega na wskazaniu stopnia zagrożenia dla realizacji zadań lub celów według poniższej skali ocen:

Wpływ	Skala	Opis
Wysoki	4	Zdarzenie uniemożliwia funkcjonowanie, koszt finansowy wysoki, znaczna utrata reputacji
Średni	3	Zdarzenie uniemożliwia realizację celów i zadań, koszt finansowy średni, średnia utrata reputacji
Niski	2	Zdarzenie utrudnia realizację celów i zadań, niski koszt finansowy, niska utrata reputacji
Znikomy	1	Zdarzenie w nieznaczny sposób wpływa na funkcjonowanie, brak kosztów finansowych oraz utraty reputacji

Określenie wpływu zdarzenia na finanse oraz wartości niematerialne, takie jak np. utrata dobrego wizerunku lub wpływ ujawnienia określonych danych na pozycję społeczną osoby, której one dotyczą

Wpływ	Skala	Opis
Wysoki	4	Wysoka wartość finansowa, wysoki wpływ na reputację
Średni	3	Średnia wartość finansowa, średni wpływ na reputację
Niski	2	Niska wartość finansowa, niski wpływ na reputację
Znikomy	1	Znikoma wartość finansowa, brak wpływu na reputację

Określenie prawdopodobieństwa wystąpienia

ryzyka polega na określeniu możliwości wystąpienia ryzyka, według poniższej skali ocen:

Prawdopodobieństwo	Skala	Opis
Wysokie	4	Istnieją powody, aby sądzić, że zdarzenie objęte ryzykiem wystąpi co najmniej raz w tygodniu.
Średnie	3	Istnieją powody, aby sądzić, że zdarzenie objęte ryzykiem wystąpi co najmniej raz w miesiącu
Niskie	2	Istnieją powody, aby sądzić, że zdarzenie objęte ryzykiem wystąpi raz na pół roku
Znikome	1	Istnieją powody, aby sądzić, że zdarzenie objęte ryzykiem wystąpi raz w ciągu roku lub nie wystąpi w ogóle.

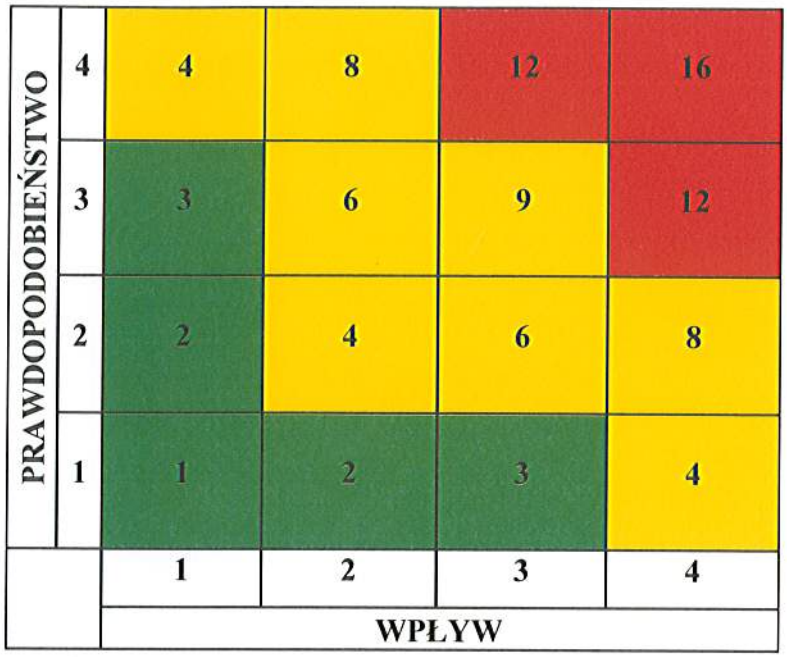
W oparciu o ocenę wpływu oraz prawdopodobieństwa ustalany jest poziom istotności ryzyka:

- **ryzyko bardzo poważne**, którego iloczyn prawdopodobieństwa wystąpienia oraz wpływu wynosi 12 lub 16 punktów;
- **ryzyko umiarkowane**, którego, którego iloczyn prawdopodobieństwa wystąpienia oraz wpływu wynosi od 6 do 9 punktów;
- **ryzyko niskie**, którego iloczyn prawdopodobieństwa wystąpienia oraz wpływu od 1 do 4.

Istotność ryzyka
Ustalona istotność ryzyka wpływa na poziom akceptacji dla danego ryzyka:

1. Poziom ryzyka jest nieakceptowany w przypadku:
   - **ryzyka bardzo poważnego**, które wymaga bezwzględnie natychmiastowej reakcji
2. Poziom ryzyka jest akceptowany warunkowo w przypadku:
   - **ryzyka umiarkowanego**, dla którego wskazana jest w reakcja kierownictwa, która może zostać przesunięta w czasie z zastrzeżeniem bieżącego monitorowania.
3. Poziom ryzyka jest akceptowany w przypadku:
   - **ryzyka niskiego,** dla którego podjęcie działań uzależnia się od decyzji Kierownictwa biorąc pod uwagę ewentualne nakłady.

Macierz ryzyka



Reakcja na ryzyko

1. W stosunku do każdego ryzyka powinno się określić rodzaj reakcji (tolerowanie, przeniesienie, unikanie, działanie).
2. Należy określić działania, które należy podjąć w celu zmniejszenia danego ryzyka do akceptowanego poziomu.
3. Zidentyfikowane i wyrażone wartością ryzyka poddaje się ocenie celem podjęcia odpowiednich decyzji, tj:
    a. **modyfikowanie (redukcja) ryzyka** – polega na obniżeniu poziomu ryzyka (np. poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszenie skutków jego wystąpienia).
    b. **dzielenie (przeniesienie) ryzyka** – polega na wykupieniu ubezpieczenia od jakiegoś zdarzenia lub scedowaniu skutków ryzyka na kontrahenta (np. podwykonawcę); należy pamiętać, że przeniesienie ryzyka nie eliminuje go. Zgodnie z przepisami ogólnego rozporządzenia o ochronie danych wykupienie ubezpieczenia nie wyeliminuje ryzyka niezastosowania się przez dany podmiot do przepisów RODO. Administrator w sytuacji, kiedy zleca innym podmiotom przetwarzanie danych, to jako podmiot decydujący o zakresie i celach tego

przetwarzania, ponosi pełną odpowiedzialność za zgodne z prawem przetwarzanie wskazanych danych.

c. **zachowanie (akceptacja) ryzyka** –świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu organizacji (zabezpieczeń), jeżeli poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka.
d. **unikanie ryzyka** – polega na unikaniu przez organizację działań, które powodują powstanie określonych typów ryzyka, np. w przypadku, gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatny do zysków

Postępowanie z ryzykiem
W praktyce reakcją na ryzyko są konkretne działania, które mogą polegać m.in. na:

- przeprowadzeniu szkolenia wewnątrz firmy lub skierowanie na szkolenie zewnętrzne,
- wprowadzenie dodatkowych środków bezpieczeństwa, które umożliwią obniżenie poziomu ryzyka lub całkowite jego wyeliminowanie
- dokonaniu zmian organizacyjnych,
- wprowadzenie nowych rozwiązań

W przypadku, gdy w kroku dotyczącym postępowania z ryzykiem podjęta zostanie decyzja o jego modyfikacji lub całkowitej eliminacji, cały proces dotyczący szacowania ryzyka powinien być powtórzony.

Dodatkowo, kiedy na etapie szacowania i oceny ryzyka ustalona zostanie wysoka wartość ryzyka, zgodnie z art. 35 RODO wymagane jest przeprowadzenie dla danego procesu przetwarzania oceny jego skutków w zakresie ochrony praw i wolności dla osób, których dane są przetwarzane.

Podczas przeprowadzania oceny skutków dla ochrony danych bierze się pod uwagę nie interesy administratora czy podmiotów przetwarzających, ale przede wszystkim ryzyko naruszenia praw i wolności osób, których dane są przetwarzane

Monitorowanie i przegląd ryzyka
Ustalone i wyrażone wartością ryzyka są na bieżąco monitorowane. Monitorowanie jest procesem ciągłym wykonywanym w toku czynności bieżących, celem ewentualnej weryfikacji realizowanych działań.

Działania korekcyjne
W przypadku stwierdzenia odstępstwa od zaplanowanych działań podejmuje się działania korygujące, które mają na celu osiągniecie zakładanych celów.

Załącznik nr 2 do Zarządzenia Wójta Gminy Boronów z dnia 05.12.2018

Arkusz analizy ryzyka dla Urzędu Gminy w Boronowie

Obszar ryzyka	Podatność	Zagrożenia	Naruszenie poufności	Naruszenie integralności	Naruszenie dostępności	Prawdopodobieństwo wystąpienia zagrożenia	Wpływ zagrożenia na działalność	Wpływ zagrożenia na utratę praw i wolności osób fizycznych (RODO)	Ryzyko	Ryzyko (RODO)	Reakcja na ryzyko
Personel	Niewystarczające szkolenia z bezpieczeństwa informacji, brak świadomości	Błąd użytkownika	x	x	x				0	0	
Personel	Nieporawne użycie oprogramowania lub sprzętu	Błąd użytkownika	x	x	x				0	0	
Personel	Praca personelu zewnętrznego lub sprzatającego bez nadzoru	Naruszeń dostępności oraz poufności danych osobowych	x		x				0	0	
Personel	Brak polityk w zakresie poprawnego użytkowania środków telekomunikacyjnych i komunikatorów	Nieautoryzowane użycie urządzeń	x	x	x				0	0	
Siedziba	Nieodpowiednie lub niestaranne użytkowanie fizycznej kontroli dostępu do budynków i pomieszczeń	Zniszczenie urządzeń lub nośników	x		x				0	0	
Siedziba	Lokalizacja na obszarach zagrożonych powodzią	Powódź			x				0	0	
Siedziba	Niestablina sieć elektryczna	Utrata zasilania			x				0	0	
Siedziba	Brak fizycznej ochrony budynku i pomieszczeń	Kradzież nośników lub dokumentów	x		x				0	0	
Organizacja	Brak lub niewystarczające zapisy dotyczące bezpieczeństwa w umowach z kontrahentami lub stronami	Nadużycie praw	x						0	0	
Organizacja	Brak regularnych audytów, przeglądów	Nadużycie praw	x	x	x				0	0	
Organizacja	Brak planów ciągłości działania	Awaria urządzenia	x		x				0	0	
Organizacja	Brak polityki korzystania z poczty elektroniczej	Błąd użytkownika, utrata informacji	x		x				0	0	
Organizacja	Brak procedur instalowania oprogramowania w systemach	Błąd użytkownika	x	x	x				0	0	
Organizacja	Brak procedur przetwarzania infomacji klasyfikowanych	Błąd użytkownika	x	x	x				0	0	
Organizacja	Brak formalnej polityki korzystania z komputerów przenośnych	Kradzież urządzenia			x				0	0	
Organizacja	Brak nadzoru nad aktywami znajdującymi się poza siedzibą	Kradzież urządzenia	x		x				0	0	
Organizacja	Brak lub niewystarczająca polityka czystego biurka i czystego ekranu	Naruszenie dostepności oraz poufności danych	x		x				0	0	
Organizacja	Brak ustanowionych mechanizmów monitorowania naruszeń bezpieczeństwa	Kradzież nośników lub dokumentów	x		x				0	0	
Sprzęt	Brak planów okresowej wymiany	Zniszczenie urządzeń lub nośników			x				0	0	
Sprzęt	Wrażliwość na wilgoć, pył, zanieczyszczenie	Pył, korozja, wychłodzenie	x		x				0	0	

Sprzęt	Wrażliwość na zmiany napięcia zasilania	Utrata zasilania			x				0	0	
Sprzęt	Niezabezpieczone urzadzenia do przetwarzania danych - drukarka na korytarzu	Kradzież dokumentów	x		x				0	0	
Sprzęt	Brak staranności przy pozbywaniu się nośników	Kradzież nośników lub dokumentów	x						0	0	
Sprzęt	Niekontrolowane kopiowanie	Kradzież nośników lub dokumentów	x		x				0	0	
Oprogramowanie	Brak wylogowania przy opuszczaniu stacji roboczej	Nadużycie praw	x						0	0	
Oprogramowanie	Pozbywanie się lub ponowne używanie nośników bez właściwego wykasowania informacji	Nadużycie praw	x						0	0	
Oprogramowanie	Skomplikowany interfejs użytkowania	Błąd użytkownika	x		x				0	0	
Oprogramowanie	Brak dokumentacji	Błąd użytkownika	x	x	x				0	0	
Oprogramowanie	Nieprawidłowe ustawienie paratmetrów	Błąd użytkownika	x	x	x				0	0	
Oprogramowanie	Brak mechanizmów identyfikacji i uwierzytelnienia takich jak uwierzytelnienie użytkownika	Fałszowanie praw	x	x	x				0	0	
Oprogramowanie	Niezabezpieczone hasłami, złe zarządzanie hasłami	Fałszowanie praw	x	x	x				0	0	
Oprogramowanie	Uruchomione zbędne usługi i oprogramowania	Nielegalne przetwarzanie danych	x		x				0	0	
Oprogramowanie	Niekontrolowane ściąganie i użytkowanie oprogramowania	Niewłaściwe funkcjowanie oprogramowania	x	x	x				0	0	
Oprogramowanie	Brak kopii zapasowych	Naruszeń dostępności oraz poufności danych osobowych poprzez uuchomienie złośliwego oprogramowania	x	x	x				0	0	
Oprogramowanie	Brak fizycznej ochrony budynków drzwi i okien	Utrata danych			x				0	0	
Oprogramowanie	Brak dowodu wysyłania lub odebrania wiadomości	Kradzież nośników lub dokumentów	x		x				0	0	
Sieć	Niezabezpieczone linie telekomunikacyjne	Odmowa działania		x	x				0	0	
Sieć	Złe łączenie kabli	Podsłuch	x	x	x				0	0	
Sieć	Pojedyńczy punkt uszkodzenia	Awaria urządzenia			x				0	0	
Sieć	Brak identyfikacji i uwierzytelnienia nadawcy i odbiorcy	Awaria urządzenia			x					0	
Sieć	Niebezpieczna architektura sieciowa	Fałszowanie praw	x		x				0	0	
Sieć	Przesyłanie hasła w jawnej postaci	Szpiegostwo zdalne	x		x				0	0	
Sieć	Nieodpowiednie zarządzanie siecią	Szpiegostwo zdalne	x						0	0	
Sieć	Niezabezpieczone połączenia z siecią publiczną	Przeciążenie systemu informacyjnego			x				0	0	
Sieć	Niezabezpieczone połączenia z siecią publiczną	Utrata dostępności, integralności i dostępności danych	x	x	x				0	0	