ZARZĄDZENIE NR 110/18

Burmistrza Gminy Żychlin

z dnia 26 października 2018 roku

w sprawie przyjęcia metodologii szacowania ryzyka dla zasobów danych osobowych w Urzędzie Gminy w Żychlinie

W celu wdrażania oraz ewaluacji środków technicznych i organizacyjnych służących zapewnieniu stopnia bezpieczeństwa odpowiednio do ryzyka wiążącego się z przetwarzaniem danych osobowych, o którym mowa w art. 32 i 35 Rozporządzeniem 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, na podstawie art.30, ust.1 ustawy z dnia 8 marca 1991r. o samorządzie gminnym (T.j. Dz. U. z 2018 r. poz. 994; zm.: Dz. U. z 2018 r. poz. 1000, poz. 1349 i poz. 1432), **zarządzam co następuje:**

§ 1. Wprowadzam do stosowania metodologię szacowania ryzyka dla zasobów danych osobowych w Urzędzie Gminy w Żychlinie stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Zobowiązuję osoby zaangażowane w procesy ochrony danych osobowych (pracowników wewnętrznych i zewnętrznych specjalistów, konsultantów lub doradców) do zapoznania się z treścią załącznika do niniejszego zarządzenia oraz stosowania jego postanowień w procesach analizy ryzyka oraz na potrzeby przygotowania oceny skutków dla ochrony danych osobowych. Stosowanie narzędzi programowych służących analizie ryzyka lub ocenie skutków dla ochrony danych jest możliwe, jeżeli wskazane narzędzia wykorzystują przyjęte w załączniku do niniejszego zarządzenia współczynniki obliczeń ryzyka.

§ 3. Wykonanie niniejszego zarządzenia powierzam inspektorowi ochrony danych.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

Grzegorz Ambroziak

RADCA PRAWNY
Waldemar Ryszard Kardasz
WA-4705

Załącznik do
Zarządzenia Nr.....
Burmistrza Gminy Żychlin
z dnia.....

METODOLOGIA SZACOWANIA RYZYKA DLA ZASOBÓW DANYCH OSOBOWYCH W URZĘDZIE GMINY W ŻYCHLINIE

1. Cel i zakres stosowania

Celem metodologii szacowania ryzyka jest identyfikacja zagrożeń i słabości w celu ich eliminacji poprzez usprawnienie bieżących lub wdrożenie nowych środków technicznych i organizacyjnych (zabezpieczeń).

W trakcie szacowania ryzyka dokonywana jest również identyfikacja ryzyka szczątkowego, podlegającego akceptacji przez organ kierowniczy ryzyka, którego usunięcie jest niemożliwe lub biznesowo nieuzasadnione.

Szacowanie ryzyka wykonywane jest przez pracowników, wewnętrznych i zewnętrznych specjalistów, konsultantów lub doradców zaangażowanych w procesy ochrony danych osobowych.

Szacowanie ryzyka obejmuje:

- dotychczasowe zasoby danych osobowych,
- jedną jednostkę organizacyjną lub grupę jednostek - w przypadku wystąpienia nowych czynników ryzyka/zagrożeń związanych z pracą danej jednostki,
- jeden zasób/grupę zasobów danych osobowych - w przypadku pojawienia się nowych zasobów podlegających ochronie, lub po zmianie uwarunkowań związanych z wykorzystaniem tych zasobów,
- problematykę współpracy z jednostkami zewnętrznymi - po wszelkich zmianach związanych z zakresem podmiotowym (umowa z nową stroną trzecią, instytucją, firmą) lub przedmiotowym (zmiana zakresu prac, itp.) związanych z tą współpracą.

2. Etapy szacowania ryzyka

1. Identyfikacja zasobów danych osobowych,
   - omówienie cech charakteryzujących zasób/zasoby,
   - sporządzenie opisów zasobów na Formularzach identyfikacji zasobów,
2. Ocena wartości zasobów oraz ich wrażliwości
   - uczestnicy oceniają poszczególne zasoby według kryterium wartości w skali (mała, średnia,

duża),

- analogicznie oceniana zostaje wrażliwość zasobu w skali (mała, średnia, duża),

- oceny wartości i wrażliwości wraz z ich uzasadnieniami, zostają zapisane w formularzach opisu zasobu,

3. Sporządzenie/aktualizacja rejestru zasobów organizacji

   - na podstawie formularzy opisu zasobów sporządzany zostaje dokument: Identyfikacja Zasobów Danych Osobowych (IZDO),

   - sporządzana zostaje tabela grupująca wszystkie zidentyfikowane zasoby,

   - dokonywana jest ocena wartości zasobów poprzez przeliczenie ocen wartości i wrażliwości według wzoru: $Wz = Wa + Wr - 1$, gdzie: Wa – ocena punktowa wartości w skali: mała – 1 pkt, średnia – 2 pkt, duża - 3 pkt, Wr – ocena punktowa wrażliwości w skali: mała – 1 pkt, średnia – 2 pkt, duża 3 pkt,

   - dokonywane jest przypisanie jednej z trzech kategorii zabezpieczeń (A,B,C), w zależności od dokonanej oceny wartości zasobu i innych jego cech charakterystycznych (dane osobowe, wykorzystanie przez inne instytucje),

   - formularze opisu zasobów stanowią załącznik do opracowanego dokumentu IZDO

4. Identyfikacja czynników ryzyka

   Pracownicy, wewnętrzni i zewnętrzni specjaliści, konsultanci lub doradcy biorą czynny udział w identyfikacji zagrożeń bezpieczeństwa danych osobowych poprzez uczestnictwo w cyklicznych spotkaniach.

   Celem spotkań jest:

   - omówienie problematyki ryzyka, źródeł zagrożeń, poziomu ich wpływu na organizację, możliwych przyczyn słabości,

   - uczestnicy sporządzają listę zagrożeń i słabości, które według nich mogą wywołać największy wpływ na funkcjonowanie organizacji; lista zagrożeń sporządzana jest na formularzu identyfikacji zagrożeń dla bezpieczeństwa danych osobowych.

5. Wyznaczenie miar ryzyka dla poszczególnych zagrożeń

   Każde zidentyfikowane zagrożenie oceniane jest za pomocą trzech miar:

   a. Poziom zagrożenia (istotność ryzyka) (Pz) jest postrzeganą miarą wpływu danego czynnika na funkcjonowanie jednostki; wysoki poziom zagrożenia dla czynnika oznacza, iż jego wystąpienie w znaczący sposób zaszkodzi funkcjonowaniu jednostki lub też posiadanym zasobom. Wartość jest zapisywana w tabeli formularza w odpowiedniej kolumnie, liczba oznacza poziom danego zagrożenia wpisywaną według zasady: mały (ograniczony) – 1 pkt, średni (poważny) – 2 pkt, duży (maksymalny) - 3 pkt,

   b. Prawdopodobieństwo wystąpienia (prawdopodobieństwo ryzyka) (Pw) jest

postrzeganą miarą prawdopodobieństwa wystąpienia poszczególnych czynników niebezpiecznych. Jego ocena może być oparta na przeszłych doświadczeniach, wcześniejszych wystąpieniach danego zagrożenia lub też na odczuciach, przeczuciach, prognozach wobec możliwości i częstotliwości wystąpienia danego zagrożenia. Wartość jest zapisywana w tabeli formularza w odpowiedniej kolumnie, liczba oznacza prawdopodobieństwo wystąpienia danego zagrożenia wpisywane według zasady: małe (ograniczone) – 1 pkt, średnie (poważne) – 2 pkt, duże (maksymalne) - 3 pkt,

c. Następstwa (N) – jest to przypisanie empirycznej skali szkodliwości w zakresie od 1 do 5, gdzie:

cyfra „1" oznacza znikomą szkodliwość,
cyfra „2" oznacza niską szkodliwość,
cyfra „3" oznacza średnią szkodliwość,
cyfra „4" oznacza dużą szkodliwość,
cyfra „5" oznacza bardzo dużą szkodliwość wystąpienia zagrożenia.

Na punktową wartość szkodliwości mogą wpływać różne czynniki. W jednym przypadku może być to strata o określonej wartości materialnej (zniszczenie wyposażenia, sprzętu komputerowego), którą łatwo oszacować, a w innym niematerialna (pogorszenie wizerunku firmy, utrata wiarygodności, utrata klientów), którą trudno w bezpośredni sposób przeliczyć na pieniądze.

Następnie wyznacza się miarę ryzyka poprzez pomnożenie wartości ***Pz * Pw * N***
W kolejnym kroku określana jest ranga zagrożenia/ryzyka w sposób następujący:
- czynniki (zagrożenia) o poziomie ryzyka (iloczynie *Pz * Pw * N*) w zakresie od 1 do 15 otrzymują rangę 3 – poziom ryzyka niski (ograniczony).
- czynniki (zagrożenia) o poziomie ryzyka (iloczynie *Pz * Pw * N*) w zakresie od 16 do 30 otrzymują rangę 2 – poziom ryzyka średni (poważny).
- czynniki (zagrożenia) o poziomie ryzyka (iloczynie *Pz * Pw * N*) w zakresie od 31 do 45 otrzymują rangę 1 – poziom ryzyka wysoki (maksymalny).

6. Sporządzenie raportu z szacowania ryzyka (RSR) zawierającego rekomendację dotyczącą akceptacji ryzyka szczątkowego (pomijalnego).
   Raport zawiera tabelaryczne zestawienie wszystkich zidentyfikowanych zagrożeń wraz z ich rangami (poziomami ryzyka). Zagrożeniom o najwyższej randze przypisywany jest wysoki priorytet, wraz z rekomendacją dotyczącą działań zabezpieczających na wypadek jego

wystąpienia. Zagrożenia, których ranga została określona została cyfrą 1 otrzymują status poziomu ryzyka „wysoki (maksymalny)" i należy przewidzieć dla nich działania zabezpieczające. Zagrożenia, których ranga została określona została cyfrą 2 otrzymują status poziomu ryzyka „średni (poważny)" i należy przewidzieć dla nich działania zabezpieczające. Zagrożenia, których ranga została określona cyfrą 3 otrzymują status poziomu ryzyka „niski (ograniczony)". Są one analizowane i rekomendowane do akceptacji przez kierownictwo w ramach identyfikacji ryzyka szczątkowego, dla których nie będą realizowane dodatkowe działania zabezpieczające.

BURMISTRZ

Grzegorz Ambroziak

3. Formularze

A. Formularz identyfikacji zasobów danych osobowych

Jednostka organizacyjna: *(dział/komórka/stanowisko pracy)*	
Osoba odpowiedzialna: *(kierownik jednostki)*	
Nazwa zasobu danych osobowych: *(wynikająca z istniejącej dokumentacji organizacyjnej, lub stosowana zwyczajowo przez pracowników jednostki)*	
Miejsce przechowywania zasobu danych osobowych: *(segregator, pokój, szafa, katalog na dysku sieciowym, katalog/baza na komputerze lokalnym, w programie/aplikacji bazodanowej)*	
Forma zasobu danych osobowych: *(dokument papierowy, dokument elektroniczny, zapis w systemie informatycznym, kartoteka, segregator itp.)*	
Inne jednostki wykorzystujące dany zasób: *(inne jednostki organizacyjne, podmioty zewnętrzne, osoby i instytucje wykorzystujące opisywany zasób informacyjny)*	
Wartość zasobu *:*	☐mała ☐średnia ☐duża
Krótkie uzasadnienie oceny wartości zasobu:	
Wrażliwość zasobu	☐mała ☐średnia ☐duża
Krótkie uzasadnienie oceny wrażliwości zasobu: *(dlaczego dany zasób jest niezbędny dla funkcjonowania jednostki?)*	
Stosowane obecnie zabezpieczenia (środki techniczne i organizacyjne): *(zabezpieczenia fizyczne, zamki, drzwi, sejfy, zabezpieczenia informatyczne, hasła, szyfrowanie danych,*	

pseudonimizajca itp)	
Ocena wystarczalności stosowanych zabezpieczeń	☐ wystarczające ☐ niewystarczające

Data i podpis osoby odpowiedzialnej/kierownictwa:

.....

B. Formularz identyfikacji zagrożeń dla bezpieczeństwa danych osobowych

Jednostka organizacyjna: *(dział/komórka/stanowisko pracy)*	

Zagrożenie	*Poziom zagrożenia (a) 1-3*	*Prawdopodo-bieństwo wystąpienia (b) 1-3*	*Następstwo 1-5*	*Miara ryzyka a*b*N*	*Ranga zagrożenia*

W kolumnie "a" wpisać liczbę określającą rangę poziomu danego zagrożenia (jego wielkości, wartości utraconych zasobów i wpływu na organizację) – im większa wartość, tym większe zagrożenie, analogicznie postąpić dla kolumny "b" : im większa wartość tym większe prawdopodobieństwo wystąpienia. „N" – następstwo wystąpienia szacujemy w skali 1-5

Data i podpis osoby odpowiedzialnej/kierownictwa:

.....