WÓJT GMINY
Skarżysko Kościelne
woj. świętokrzyskie

ZARZADZENIE NR 171/2019
z dnia 31 grudnia 2019 roku
WÓJTA GMINY SKARŻYSKO KOŚCIELNE

w sprawie: wprowadzenia „Metodyki szacowania ryzyka naruszenia praw lub wolności osób fizycznych w Urzędzie Gminy Skarżysko Kościelne"

Na podstawie art. 24 ust. 1 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) z dnia 27 kwietnia 2016 r. (Dz.Urz.UE.L Nr 119) oraz art. 31 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (tj. Dz.U. z 2019 poz. 506)

zarządzam, co następuje:

§ 1. Wprowadza się do stosowania „Metodykę szacowania ryzyka naruszenia praw lub wolności osób fizycznych w Urzędzie Gminy Skarżysko Kościelne", która stanowi załącznik nr 1 do niniejszego zarządzenia.

§ 2. Powołuje się zespół ds. szacowania ryzyka w następującym składzie:
1. Sekretarz Gminy – przewodniczący zespołu,
2. Inspektor Ochrony Danych – członek zespołu,
3. Administrator Systemów Informatycznych – członek zespołu.

§ 3. Nadzór nad wykonaniem zarządzenia powierza się Sekretarzowi Gminy.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT
mgr Jacek Bryzik

WÓJT GMINY
Skarżysko Kościelne
woj. świętokrzyskie

Załącznik Nr 1
do Zarządzenia Nr 171/2019
z dnia 31 grudnia 2019r.

Metodyka szacowania ryzyka naruszenia praw lub wolności osób fizycznych w Urzędzie Gminy Skarżysko Kościelne

Zatwierdził:	Data:
WÓJT *mgr Jacek Bryzik* Administrator Danych Osobowych	31 grudnia 2019 rok

1. Wprowadzenie

Celem niniejszego dokumentu jest ustanowienie metody szacowania ryzyka naruszenia praw lub wolności osób fizycznych w Urzędzie Gminy Skarżysko Kościelne. Prawdopodobieństwo i wagę ryzyka określono poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych.
Jako podstawę wykonania analizy ryzyka przyjmuje się następujące dokumenty:

- PN-ISO/IEC 27001:2017 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji,
- PN-ISO/IEC 27002:2017 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji,
- PN-ISO/IEC 27005:2014 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji,
- Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych - rekomendacje i zalecenia Komitetu Rady Ministrów ds. Cyfryzacji.

Niniejsza metoda w zakresie szacowania ryzyka przyjmuje podejście procesowe. Za proces należy uznawać każdą czynność wymienioną w rejestrze czynności przetwarzania danych osobowych.

Definicje

1) administrator merytoryczny – osoba nadzorująca przetwarzanie informacji;
2) administrator techniczny – osoba właściwa w sprawach prawidłowego funkcjonowania sieci/systemu/infrastruktury;
3) akceptacja ryzyka – decyzja Wójta o zaniechaniu działań mających na celu zmianę poziomu ryzyka;
4) analiza ryzyka – systematyczne podejście mające na celu zidentyfikowanie źródeł ryzyka i przypisanie zidentyfikowanym ryzykom wartości;
5) dostępność informacji – właściwość polegającą na tym, że informacja jest możliwa do wykorzystania przez uprawniony podmiot na jego żądanie, w założonym czasie;
6) identyfikowanie ryzyka – proces znajdowania, zestawiania i charakteryzowania przyczyn ryzyka;
7) incydent – pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji;
8) informowanie o ryzyku – wymiana lub dzielenie się informacją o ryzyku między kierownikami jednostek organizacyjnych/komórek organizacyjnych;
9) integralność informacji – właściwość polegającą na tym, że informacja nie została zmodyfikowana w sposób nieuprawniony;
10) końcowy poziom ryzyka – poziom ryzyka pozostający po procesie postępowania z ryzykiem;

11) podatność – słabość zabezpieczenia, która może być wykorzystana przez co najmniej jedno zagrożenie;
12) postępowanie z ryzykiem – proces wyboru i wdrażania środków sterowania ryzykiem mających na celu zmianę wartości poziomu ryzyka;
13) poziom ryzyka – produkt operacji na wartości przypisanej skutkowi i wartości związanej z prawdopodobieństwem zaistnienia zdarzenia powodującego skutek,
14) poufność informacji – właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom, do ustalonego celu;
15) ryzyko szczątkowe – ryzyko, którego poziom nie przekracza akceptowanej wartości;
16) skutek – negatywna zmiana w odniesieniu do zaplanowanego poziomu miernika celu w wyniku oddziaływania zagrożenia;
17) szacowanie ryzyka – całościowy proces analizy i oceny ryzyka;
18) zagrożenie – potencjalna przyczyna niepożądanego oddziaływania.

2. Procedura szacowania ryzyka

2.1. Identyfikowanie procesów

Identyfikacja procesów zawarta jest w następujących dokumentach:
„Rejestr czynności przetwarzania danych osobowych"
„Rejestr kategorii czynności przetwarzania"

2.2. Identyfikowanie zagrożeń

Identyfikowanie zagrożeń przeprowadza się w poszczególnych grupach ryzyk, uwzględniając zaangażowane w proces aktywa, cele przetwarzania oraz skutki.
Zidentyfikowanym zagrożeniom należy przypisać wartość ich wpływu na dostępność, integralność i poufność danych w kontekście danej grupy ryzyk.
Początkową identyfikację zagrożeń i analizę ryzyka przeprowadza administrator merytoryczny w porozumieniu z administratorem technicznym i inspektorem danych osobowych.
Identyfikację zagrożeń prowadzi się okresowo lub *ad hoc*.
Identyfikacja *ad hoc* dokonywana jest w przypadku planowania nowych czynności przetwarzania lub zaobserwowania zaistnienia zagrożenia, którego okres trwania jest krótszy od okresowej identyfikacji zagrożeń, a zwłoka w identyfikacji miałaby istotne znaczenie dla ochrony danych. Identyfikacją *ad hoc* dokonywana jest także w przypadku wystąpienia incydentu teleinformatycznego, którego skutkiem była utrata bezpieczeństwa informacji mająca charakter katastrofalny. W szczególności identyfikację zagrożeń przeprowadza się przed oddaniem systemu do eksploatacji.

Źródła potencjalnych zagrożeń powinny być zgłaszane w każdym momencie, przez każdego użytkownika.

2.3. Identyfikowanie istniejących zabezpieczeń

W celu oszacowania ryzyka, należy również zidentyfikować istniejące już zabezpieczenia, które skutecznie obniżając prawdopodobieństwo wystąpienia wpływają na obniżenie poziomu ryzyka. Podczas identyfikacji wdrożonych zabezpieczeń poszczególnym zabezpieczeniom

należy przypisać wartość określającą skuteczność ich oddziaływania na dostępność, integralność i poufność danych.

2.4. Analiza ryzyka

Analizy ryzyk dokonuje osoba lub zespół osób wyznaczonych przez Wójta. Po zakończeniu procesu analizy i parafowaniu przez administratora technicznego, administratora merytorycznego i Inspektora ochrony danych, odpowiedzialnych za bezpieczeństwo systemów teleinformatycznych i zakres merytoryczny informacji, wyniki zatwierdza Wójt. Na analizę ryzyka składają się:

- szacowanie następstw,
- szacowanie prawdopodobieństwa incydentu,
- określenie poziomu ryzyka.

2.4.1. Szacowanie prawdopodobieństwa incydentu

Szacowanie prawdopodobieństwa incydentu ma na celu ustalenie częstotliwości z jaką mogą pojawiać się określone incydenty. Pod uwagę powinny być brane następujące okoliczności:

- doświadczenie szacującego oraz statystyki dotyczące podobnych zdarzeń,
- w przypadku zagrożeń antropogennych (których udziałem jest człowiek) atrakcyjność aktywu lub efekt skutku wywołującego incydent,
- dla zagrożeń o charakterze przypadkowym położenie geograficzne, warunki pogodowe itp., które mogą oddziaływać na powstawanie błędnych działań użytkowników, zasobów informacyjnych lub systemów teleinformatycznych,
- podatność.

2.4.2. Określanie poziomu ryzyka

Określanie poziomu ryzyka polega na przypisaniu danemu zagrożeniu prawdopodobieństwa oddziaływania oraz ustaleniu wpływu zaistnienia zagrożenia na:

1) dostępność informacji;
2) integralność informacji;
3) poufność informacji,

a następnie wyznaczeniu poziomu ryzyka.

Poziom ryzyka wyznacza się według następującego wzoru:

$$R_p = P \times (S_d + S_i + S_p)$$

gdzie:

R_p – pierwotny poziom ryzyka,

P – wartość przypisana prawdopodobieństwu zaistnienia zagrożenia,

$$P \in \{0,1,2,3,4\}$$

gdzie:

0 – zdarzenie nieprawdopodobne (zagrożenie nie występuje),

1 – zdarzenie prawie nieprawdopodobne,

2 – zdarzenie mało prawdopodobne,

3 – zdarzenie wysoce prawdopodobne,

4 – zdarzenie niemal pewne.

S_d – wartość przypisana skutkowi dla dostępności informacji,

S_i – wartość przypisana skutkowi dla integralności informacji,

S_p – wartość przypisana skutkowi dla poufności informacji,

$$(S_d, S_i, S_p) \in \{0,1,2,3,4\}$$

gdzie:

0 – zdarzenie nie powoduje skutku (brak podatności),

1 – zdarzenie wywołuje niewielki skutek,

2 – zdarzenie wywołuje znaczący skutek,

3 – zdarzenie wywołuje bardzo znaczący skutek,

4 – zdarzenie wywołuje skutek katastrofalny.

Podczas doboru wartości przypisywanej prawdopodobieństwu wystąpienia zagrożenia należy przyjąć następujące wartości:

0 - wystąpienie zagrożenia jest **wysoce nieprawdopodobne** w odniesieniu do analizowanej czynności, lub charakter zagrożenia jest **nieadekwatny** do specyfiki czynności;

1 - zagrożenie występuje rzadziej niż **co dziesięć lat** lub brak jest informacji by zagrożenie występowało;

2 - zagrożenie występuje **co kilka lat** lub zagrożenie wystąpiło w pojedynczych przypadkach;

3 - zagrożenie może wystąpić **kilka razy w roku**;

4 - zagrożenie wystąpiło **wielokrotnie w ciągu roku**.

Podczas doboru wartości przypisywanej skutkowi dla odpowiednich atrybutów bezpieczeństwa informacji należy przyjąć następujące zasady:

Dla skutku utraty dostępności [Sd]:

0 - zdarzenie nie powoduje skutku (brak podatności);

1 - czas utraty dostępności informacji lub usług systemu, spowodowany wystąpieniem zagrożenia, **mieści się w akceptowalnym okresie** czasu, a przywrócenie pełnego dostępu do informacji lub usług systemu **nie wiąże się z dodatkowymi kosztami**;

2 - czas utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, **mieści się w akceptowalnym okresie czasu**, ale przywrócenie dostępu do informacji wiąże się z **dodatkowymi kosztami**;

3 - czas utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, **znacząco nie mieści się w akceptowalnym okresie czasu**;

4 - czas utraty dostępności informacji lub usług systemu, spowodowany zagrożeniem, **wielokrotnie przekracza założony czas** lub jeżeli spowodowana zagrożeniem utrata dostępności informacji **jest nieodwracalna**.

Dla skutku utraty integralności [Si]:

0 - zdarzenie nie powoduje skutku (brak podatności),

1 - spowodowana zagrożeniem utrata integralności informacji **jest łatwo wykrywalna** i przywrócenie integralności **nie powoduje nadmiernych kosztów**,

2 - spowodowana zagrożeniem utrata integralności informacji **jest trudno wykrywalna** i informacja taka może zostać **użyta w procesach decyzyjnych**, jednak **istnieje możliwość skorygowania decyzji**,
3 - spowodowana zagrożeniem utrata integralności informacji jest **trudno wykrywalna** i informacja taka może zostać użyta w procesach decyzyjnych i **nie istnieje możliwość skorygowania decyzji**,
4 - spowodowana zagrożeniem utrata integralności informacji może okazać się **niewykrywalna** należy przyjąć S_i=4.

Uwaga:
W praktyce może pojawić się problem korelacji atrybutu dostępności z atrybutem integralności, przyjmujący postać dylematu – czy informacja zniekształcona poprzez utratę integralności jest informacją dostępną, czy też wraz z utratą integralności nastąpiła utrata dostępności. Na potrzeby niniejszej analizy należy przyjąć, że utrata integralności informacji nie powoduje automatycznej utraty dostępności. Atrybuty dostępności i integralności informacji należy rozpatrywać rozłącznie.

Dla skutku utraty poufności [Sp]:
0 - zdarzenie nie powoduje skutku (brak podatności),
1 - utrata poufności dotyczy **zwykłych kategorii danych osobowych** oraz odnosi się do **pojedynczych przypadków**,
2 - utrata poufności dotyczy **zwykłych kategorii danych osobowych** oraz odnosi się do **licznych przypadków**,
3 - utrata poufności dotyczy **szczególnych kategorii danych osobowych** oraz odnosi się do **pojedynczych przypadków**,
4 - utrata poufności dotyczy **szczególnych kategorii danych osobowych** oraz odnosi się do **licznych przypadków**.

2.5. Ocena ryzyka
Ocena ryzyka polega na porównaniu wyznaczonych poziomów ryzyka z ustalonymi kryteriami akceptowania ryzyka i umożliwia ustalenie priorytetów.
Ryzyka, dla których wartość pierwotnego poziomu, jest niższa lub równa 20% poziomu maksymalnego ($R_p \leq 9{,}6$) uznaje się *a priori* za ryzyka szczątkowe, które nie podlegają procedurze postępowania z ryzykiem. Ryzyka dla których poziom przekracza 20% poziomu ryzyka maksymalnego ($R_p > 9{,}6$), podlegają procedurze postępowania z ryzykiem.

2.6. Postępowanie z ryzykiem
Ryzyka, które na poziomie oceny nie zostały uznane za ryzyka szczątkowe, podlegają procedurze postępowania z ryzykiem. Postępowanie z ryzykiem może polegać na:
1. sterowaniu ryzykiem poprzez zastosowanie zabezpieczenia;
2. unikaniu ryzyka;
3. przeniesieniu ryzyka;
4. akceptacji ryzyka mimo, że jego poziom przekracza poziom ryzyka szczątkowego.

2.6.1. Sterowanie ryzykiem

Sterowanie ryzykiem ma na celu ograniczanie poziomu ryzyka końcowego poprzez zastosowanie zabezpieczenia, dobranego adekwatnie do charakteru tego ryzyka.
Na etapie postępowania z ryzykiem dokonuje się ponownego estymowania poziomu ryzyka z uwzględnieniem zastosowanych zabezpieczeń. Przeliczenie dokonywane jest według wzoru:

$$R_k = Px\left(\frac{S_d}{\Sigma C_d} + \frac{S_i}{\Sigma C_i} + \frac{S_p}{\Sigma C_p}\right)$$

gdzie:
R_k – końcowy poziom ryzyka,
P, Sd, Si, Sp zdefiniowane w pkt. 2.4.2,
C – skuteczność pojedynczego zabezpieczenia,

$$(C_d, C_i, C_p) \in \{1,2,3,4\}$$

gdzie:
1 – brak zabezpieczenia,
2 – zabezpieczenie ogranicza poziom ryzyka,
3 – zabezpieczenie w istotny sposób ogranicza poziom ryzyka,
4 – zabezpieczenie w bardzo istotny sposób ogranicza poziom ryzyka.

Podczas doboru wartości wskaźnika skuteczności pojedynczego zabezpieczenia należy przyjąć następujące zasady:
1 – **brak możliwości** zastosowania zabezpieczenia lub zastosowanie zabezpieczenia jest **niecelowe** (np. w przypadku S=0),
2 – zabezpieczenie powoduje obniżenie skutku $S_{d,i,p}$ **o jeden** stopień,
3 – zabezpieczenie powoduje obniżenie skutku $S_{d,i,p}$ **o dwa** stopnie,
4 – zabezpieczenie powoduje obniżenie skutku $S_{d,i,p}$ **o co najmniej trzy** stopnie.

Metodyka zakłada zastosowanie więcej niż jednego zabezpieczenia. Zastosowanie kolejnych zabezpieczeń podnosi ich sumaryczną skuteczność (ΣC) zależnie od stopni obniżenia skutków, jednak ich suma nie może przyjmować wartości większej niż 4.

$$\Sigma C = (C1+C2+C3-2) \text{ ale nie więcej niż } 4$$

przykładowo:
- dla 3 zabezpieczeń o wskaźnikach skuteczności 2, 2 i 1 ich sumaryczny wskaźnik skuteczności wyniesie 3;
- dla 3 zabezpieczeń o wskaźnikach skuteczności 3, 3 i 2 ich sumaryczny wskaźnik skuteczności wyniesie 4;

Zastosowanie zabezpieczenia musi uwzględniać wpływ tegoż zastosowanego zabezpieczenia na pozostałe atrybuty bezpieczeństwa i samo w sobie może stanowić czynnik ryzyka. Przykładowo: zastosowanie zabezpieczenia ograniczającego ryzyko utraty poufności może spowodować podniesienie ryzyka utraty dostępności. W takim przypadku należy powrócić do oszacowania początkowego poziomu ryzyka z uwzględnieniem zastosowanego zabezpieczenia.

2.6.2. Unikanie ryzyka

Unikanie ryzyka może przyjąć formę rezygnacji z przyjętych w organizacji metod na rzecz innych, bezpieczniejszych, które zapewnią tą samą funkcjonalność, np. zamiast przesyłania plików jawnym e-mailem można przyjąć formę wymiany plików przez bezpieczny serwer sftp.

2.6.3. Przeniesienie ryzyka

W przypadku realizacji zadań publicznych przeniesienie ryzyka, co do zasady, może mieć zastosowanie, np. w formie ubezpieczenia. Wydaje się jednak, że w kontekście bezpieczeństwa danych osobowych, obniżenie ryzyka skutków finansowych nie ma znaczenia.
Natomiast zlecenie pewnych czynności np. niszczenie nośników danych, firmie zewnętrznej profesjonalnie zajmującej się taką działalnością, może stanowić element przeniesienie ryzyka.

2.6.4. Akceptacja ryzyka

W wyniku przeliczenia poziomów ryzyk uzyskuje się wartość końcową poziomu ryzyka. Ryzyka, dla których końcowy poziom ryzyka jest niższy lub równy 20% poziomu maksymalnego ($R_k \leq 9,6$) podlegają automatycznej akceptacji, ale pozostają pod nadzorem w celu ich monitorowania. Ryzyka dla których poziom zawiera się w przedziale $9,6 < R_k \leq 24$ podlegają akceptacji według zasad ustalonych w niniejszym dokumencie lub dokonywana jest ich ponowna analiza. Ryzyka dla których poziom ryzyka jest wysoki (większy od 50% poziomu maksymalnego; $R_k > 24$), przedstawiane są Wójtowi do dalszego postępowania, zgodnie z 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 (ogólne rozporządzenie o ochronie danych).

3. Raportowanie i terminy działań w szacowaniu ryzykiem

Raportowaniu podlegają szacowania ryzyka sporządzone odrębnie dla każdego zachodzącego w jednostce procesu w którym przetwarzane są dane osobowe. Raportowanie w zakresie analizy ryzyka odbywa się w następujący sposób:

1) szacowanie ryzyka przeprowadzane jest nie rzadziej niż raz na 3 lata, chyba że przepis szczególny stanowi inaczej oraz w każdej sytuacji mającej wpływ na poziom ryzyka,
2) dokonywane jest przez Zespół powołany w celu szacowania ryzyka naruszenia praw i wolności osób w procesie przetwarzania,
3) szacowanie ryzyka przekazywane jest Wójtowi wraz z informacją o ryzykach do akceptacji lub opinii wprowadzenia nowych zabezpieczeń.

Dopuszcza się grupowanie zachodzących procesów przetwarzania danych osobowych.

4. Monitorowanie i przegląd ryzyka

Należy monitorować i utrzymywać bezpieczeństwo poprzez przeglądy ryzyk. Mogą one być planowane - okresowe analizy ryzyka oraz nieplanowane – jako reakcja na często zgłaszane incydenty związane z bezpieczeństwem informacji.

Pracownicy odpowiedzialni za funkcjonowanie systemu bezpieczeństwa informacji i ochrony danych osobowych na bieżąco monitorują jego funkcjonowanie.