METODYKA OCENY SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH

MYŚLENICKI OŚRODEK KULTURY I SPORTU

ul. Piłsudskiego 20,

32-400 Myślenice

NIP: 6811353451, REGON: 000284888

Zatwierdzenie dokumentu:		01.02.2019 r.
sporządził:	Krzysztof Dybeł	.....
zatwierdził:	Administrator Danych	.....

INSPEKTOR OCHRONY DANYCH OSOBOWYCH
inż. Krzysztof Dybeł

p.o. Dyrektora
Myślenickiego Ośrodka Kultury i Sportu
mgr Piotr Szewczyk

SPIS TREŚCI

1. TERMINY I DEFINICJE

Terminologia obowiązująca w niniejszym dokumencie została zdefiniowana w „Polityce bezpieczeństwa danych osobowych" (BA01-Polityka bezpieczeństwa danych osobowych). Pozostałe terminy zostały zdefiniowane poniżej:
Aktyw informacyjny – wszystko co ma wartość dla organizacji oraz stanowi istotny element przetwarzania informacji;
Poufność – właściwość zapewniającą, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym podmiotom lub osobom fizycznym;
Integralność – właściwość polegającą na tym, że aktyw teleinformacyjny nie został zmodyfikowany w sposób nieuprawniony;
Dostępność – właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;
Grupa informacji (zasób informacyjny) – nieformalny zbiór informacji podobnych pod kątem zawartości informacyjnej i jej wartości dla organizacji;
Klasyfikacja informacji – Dokument systemowy dokonujący klasyfikacji występujących w organizacji informacji, aktywów i zasobów informacyjnych, odzwierciedlający potrzeby, priorytety oraz oczekiwany poziom ochrony przy ich przetwarzaniu;
Podatność – cecha zasobu powodująca, że zasób jest narażony na działanie jednego lub wielu zagrożeń (np. podatnością serwerowni jest drewniana podłoga, zagrożeniem w tym przykładzie – pożar);
Punkt krytyczny – potencjalny negatywny czynnik poddawany ocenie będący podstawą do wyznaczenia ryzyka (zagrożenie lub podatność). Punkt krytyczny jest scharakteryzowany następującymi atrybutami:

- prawdopodobieństwo realizacji punktu krytycznego,
- skutek realizacji punktu krytycznego,
- wykrywalność;

Zabezpieczenie – rozwiązanie techniczne lub organizacyjne minimalizujące ryzyko;
Zagrożenie – niepożądane działanie lub sytuacja dotycząca aktywu lub grupy aktywów, która może niekorzystnie wpłynąć na prawidłowość oraz bezpieczeństwo procesów realizowanych w organizacji.

2. CELE METODYKI

„Metodyka oceny skutków dla ochrony danych osobowych" służy realizacji wymogów prawnych odnoszących się do przestrzegania praw i wolności osób których dane osobowe są przetwarzane w Myślenickim Ośrodku Kultury i Sportu.
„Metodyka oceny skutków dla ochrony danych osobowych" ma umocowanie w ROZPORZĄDZENIU 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 – artykuł 35.
„Metodyka oceny skutków dla ochrony danych osobowych" jest narzędziem zarządczym używanym do kształtowania procesów i zasad przetwarzania danych osobowych w Myślenickim Ośrodku Kultury i Sportu.
Strategicznymi celami „Metodyki oceny skutków dla ochrony danych osobowych" są:

- zapewnienie przetwarzania danych osobowych zgodnie z wymogami prawa w zakresie ochrony danych osobowych,
- ocena występujących czynników, mających wpływ na ochronę danych, które są przetwarzane w Myślenickim Ośrodku Kultury i Sportu
- przyjęcie modelu dokumentowania działań wynikających z prowadzonych ocen ryzyka naruszenia ochrony danych osobowych.

Powyższe cele będą realizowane poprzez:

- wprowadzenie spójnej metody pozwalającej ocenić skutki naruszenia ochrony danych osobowych,

- klasyfikację aktywów,
- identyfikację zagrożeń,
- analizę oddziaływania oraz prawdopodobieństwa,
- określenie kryteriów oceny i akceptacji,
- dokumentowanie procesu oceny.

3. ZAKRES STOSOWANIA METODYKI OCENY SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH

Niniejsza metodyka określa tryb postępowania w przypadku:

a) Zidentyfikowania ryzyk w oparciu o analizę zagrożeń oraz zabezpieczeń organizacyjnych, fizycznych i technicznych w organizacji – realizowana minimum raz w roku lub w przypadku mających znaczenie zmian organizacyjnych, zmian w systemach informatycznych;
b) Zidentyfikowania ryzyk w oparciu o zdarzenia mające charakter incydentów, niezgodności czy też podatności.

4. METODOLOGIA OCENY SKUTKÓW DLA OCHRONY DLA OCHRONY DANYCH OSOBOWYCH

4.1. Założenia

Skuteczna ocena skutków w obszarze ochrony danych osobowych wymaga spełnienia następujących warunków:

- zapewnienia powtarzalności i porównywalności wyników,
- uwzględnienia prawdopodobieństwa wystąpienia zdarzenia (zagrożenia),
- uwzględnienia konsekwencje mogące wyniknąć jego realizacji zdarzenia (skutków),
- uwzględnienia efektywności funkcjonujących zabezpieczeń,
- wpływających na prawdopodobieństwo zajścia zdarzeń,
- wpływających na późniejsze ewentualne konsekwencje realizacji zdarzenia.

4.2. Podstawy oceny skutków dla ochrony danych osobowych.

Pierwszym elementem jest analiza zidentyfikowanych ryzyk, w której oceniamy prawdopodobieństwo wystąpienia zagrożenia oraz skutków, jakie zagrożenie może wywołać.
Drugim elementem jest rejestracja ryzyk w kartach oceny ryzyka, które podlegają bieżącej ocenie i monitorowaniu (nie rzadziej niż raz na rok). Karta ryzyka jest również dokumentem opisującym sposoby postępowania z ryzykiem, zadania mające na celu obniżenie ryzyka, kroki jakie należy podjąć w przypadku, gdy ryzyko się zmaterializuje.
Trzecim elementem jest cykliczność postępowania z ryzykiem. Ryzyko powinno zostać przeanalizowane ponownie w ciągu 12 miesięcy.

4.3. Identyfikacja przedmiotu oceny ryzyka

Identyfikacja przedmiotu oceny skutków naruszenia ochrony danych osobowych odbywa się w oparciu o:

a) rejestr czynności przetwarzania danych osobowych;
a) klasyfikację procesów przetwarzania danych osobowych;
b) kontekst organizacji;

które oprócz dostarczenia katalogu środków oraz procesów przetwarzania informacji wskazują, jaka jest wartość danego elementu/obszaru/zagadnienia.

5. Opis metody oceny skutków dla ochrony danych osobowych

5.1. Klasyfikacja procesów przetwarzania danych

Klasyfikując procesy przetwarzania danych, które będą podlegały ocenie skutków brane są pod uwagę zasoby zawierające dane osobowe oraz procesy związane z przetwarzaniem danych osobowych.
Klasyfikacja zasobów uwzględnia kto jest właścicielem/gestorem danego zasobu informacyjnego lub procesu związanego z przetwarzaniem danych osobowych oraz jakie wymagania bezpieczeństwa zidentyfikowano dotychczas w celu jego zabezpieczenia.
Zidentyfikowane procesy przetwarzania poddaje się analizie pod względem ich istotności w organizacji. Określenie ich wartości dla działalności organizacji następuje poprzez przydzielenie im odpowiednich ocen w obszarach P-Poufności, D-Dostępności, I-Integralności.

Określenie poziomu poufności informacji	
1	Informacje zawierają dane identyfikujące osobę fizyczną ale identyfikacja wymagała by niewspółmiernych środków dla zidentyfikowania (np. samo imię oraz nazwisko)
2	Informacje chronione przede wszystkim przepisami o ochronie danych osobowych
3	Dane o charakterze szczególnym w rozumieniu art. 9 RODO.

Określenie poziomu dostępności informacji	
1	Informacje, które są konieczne do realizacji zadania, a przerwa w dostępie do nich może wynosić 7-30 dni roboczych.
2	Informacje, które są konieczne do realizacji zadania, a przerwa w dostępie do nich nie może być dłuższa niż 3-7 dni roboczych.
3	Informacje muszą być dostępne w sposób nieprzerwany, brak dostępu może w skrajnych okolicznościach skutkować sankcjami karnymi lub odszkodowawczymi.

Określenie poziomu integralności informacji	
1	Naruszenie integralności informacji jest łatwe do wykrycia i naprawienia, skutki wywołane nieprawidłową informacją są łatwe do przewidzenia i naprawienia.
2	Naruszenie integralności informacji jest możliwe do wykrycia i naprawienia, skutki wywołane wadliwą informacją są możliwe do skorygowania, wymaga to jednak pewnego wkładu pracy i/lub wiąże się z poniesieniem niewielkich nakładów finansowych
3	Naruszenie integralności informacji jest trudne lub wręcz niemożliwe do naprawienia, skutki wywołane wadliwą informacją wiążą się z poważnymi sankcjami (np. odszkodowawczymi lub karnymi), usunięcie lub skorygowanie skutków wiąże się z poniesieniem znaczących nakładów finansowych

5.2. Identyfikacja zagrożeń

Dla każdego procesu przetwarzania danych osobowych określa się podatności i zagrożenia mogące się z mini wiązać. W analizie bierzemy pod uwagę trzy grupy zagrożeń dla zasobów informacyjnych organizacji, które rozważamy w kontekście określenia ryzyka związanego z przetwarzaniem informacji:

a) zagrożenia dla poufności informacji;
c) zagrożenie dla integralności (nienaruszalność):
   - dla informacji – właściwość polegająca na tym, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   - dla systemu – właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od manipulacji (nieautoryzowanych działań - celowych lub przypadkowych);

d) zagrożenie dla dostępności informacji.

Identyfikacja zagrożeń musi być zbieżna z klasyfikacją informacji. W celu zapewnienia, że wszystkie ewentualne zagrożenia zostały zidentyfikowane, można posłużyć się „Listą kontrolną ryzyk".

5.3. Oddziaływania zagrożeń na ochronę danych osobowych

Badane procesy przetwarzania danych analizowane są pod kątem wpływu typowych podatności oraz wynikających z nich zagrożeń. Zagrożenia analizowane są pod kątem możliwości utraty poufności, integralności i dostępności.
Każde zagrożenie oceniane jest w skali pięciostopniowej, według kryteriów uwzględniających jego potencjalne następstwa (oddziaływanie).
Kryteria oceny znajdują się w poniższej tabeli.

Poziom potencjalnego oddziaływania zmaterializowanego zdarzenia			
Poziom	Skutki finansowe	Odpowiedzialność za zaistnienie incydentu	Reputacja
1	od 100 zł do 1000 zł	Nie ma naruszenia przepisów prawa	Ubogie informacje w mediach lokalnych lub regionalnych
2	od 1000 zł do 10.000 zł	Naruszenie przepisów prawa - brak sankcji	Ograniczone informacje w mediach lokalnych lub regionalnych
3	od 10.000 zł do 100.000 zł	Złamanie przepisów prawa - odpowiedzialność służbowa	Pewne informacje w mediach lokalnych lub regionalnych
4	od 100.000 zł do 250.000 zł	Złamanie przepisów prawa - odpowiedzialność służbowa lub finansowa	Pewne informacje w mediach ogólnokrajowych
5	od 250.000 zł	Złamanie przepisów prawa - odpowiedzialność karna, ograniczenie lub pozbawienie wolności	Doniesienia medialne w całym kraju

5.4. Prawdopodobieństwa wystąpienia zagrożeń

Każde z ocenianych zagrożeń dla grup aktywów informacyjnych/procesów jest oceniane pod kątem prawdopodobieństwa wystąpienia. Skala oceny jest pięciostopniowa. Prawdopodobieństwo wystąpienia ryzyka oceniamy uwzględniając funkcjonujące zabezpieczenia. Kryteria oceny znajdują się w poniższej tabeli.

Prawdopodobieństwa wystąpienia zdarzenia	
1	Zdarzenie, którego zaistnienie jest wysoce nieprawdopodobne lub prawdopodobne tylko teoretycznie.
2	Zdarzenie, którego zaistnienie jest mało prawdopodobne, być może raz na 3 lata.
3	Wydarzenie, którego zaistnienie jest względnie prawdopodobne, być może raz w roku.
4	Wydarzenie, którego zaistnienie jest dość prawdopodobne i można się go spodziewać kilka razy w roku.
5	Wydarzenie wysoce prawdopodobne, którego można się spodziewać raz w miesiącu lub częściej.

5.5. Waga ryzyka

Waga ryzyka określana jest w pięciostopniowej skali:
Bardzo Małe (BM), Małe(M), Średnie(S), Duże (D), Bardzo Duże(BD).
Wagę ryzyka ustala się na podstawie macierzy ryzyka, w której przyporządkowuje się ocenę prawdopodobieństwa do wpływu, jakie potencjalnie ryzyko niesie ze sobą.

Macierz ryzyka					
Prawdopodobieństwo / Skutek	1	2	3	4	5
1	BM	BM	M	S	S
2	BM	M	S	S	D
3	M	S	S	D	D
4	S	S	D	D	BD
5	S	D	D	BD	BD

5.6. Kryteria akceptacji

Otrzymane przyporządkowanie – interpretuje się według tabeli „Dopuszczalności ryzyka".

Dopuszczalność ryzyka		
BM	BARDZO MAŁE (DOPUSZCZALNE)	Nie jest konieczne prowadzenie żadnych działań.
M	MAŁE (DOPUSZCZALNE)	Zaleca się rozważenie możliwości dalszego zmniejszania poziomu ryzyka lub zapewnienie, że ryzyko pozostaje najwyżej na tym samym poziomie.
S	ŚREDNIE (DOPUSZCZALNE)	Zaleca się zaplanowanie i podjęcie działań zmniejszających poziom ryzyka.
D	DUŻE (NIEDOPUSZCZALNE)	Jeżeli ryzyko jest związane z przetwarzaniem danych, działania w celu jego zmniejszenia należy podjąć natychmiast. Planowanego przetwarzania nie należy rozpoczynać do czasu zmniejszenia ryzyka do poziomu dopuszczalnego.
BD	BARDZO DUŻE (NIEDOPUSZCZALNE)	Ryzyko na poziomie krytycznym; działania obniżające ryzyko należy podjąć natychmiast, w skrajnym wypadku należy zaprzestać przetwarzania danych.

5.7. Karta ryzyka naruszenia ochrony danych osobowych

Karta ryzyka służy do dokumentowania analizy ryzyka. Dokumentuje ryzyko wystąpienia zdarzenia negatywnie oddziałującego na bezpieczeństwo danych osobowych w odniesieniu do aktywy informacyjnego/procesu. Dla każdego aktywu informacyjnego/procesu należy sporządzana jest osobna karta.
W karcie zapisujemy informacje dotyczące zasobu, jego podatność, istniejące zabezpieczenia (techniczne i organizacyjne), wynikające z analizy ryzyka zidentyfikowane zagrożenia, które realnie mogą mieć wpływ na bezpieczeństwo danych osobowych.

5.8. Rejestr ryzyk naruszenia ochrony danych osobowych

Za prowadzenie rejestru ryzyk odpowiedzialny jest Administrator Danych. Administrator Danych może powierzyć prowadzenie rejestru wskazanej osobie. Rejestr zidentyfikowanych ryzyk ma na celu ewidencjonowanie kart analizy ryzyka ze szczególnym uwzględnieniem ryzyk niedopuszczalnych oraz statusu działań mających na celu ograniczenie niedopuszczalnego ryzyka.

5.9. Raport z oceny ryzyka naruszenia ochrony danych osobowych

Raport z oceny naruszenia ochrony danych osobowych dokumentowany jest w „Karcie ryzyka". W celu ułatwienia monitorowania zidentyfikowanych ryzyk naruszenia ochrony, ryzyka na poziomie „Duże" i „Bardzo Duże" odnotowuje się w rejestrze ryzyk.

5.10. Plan postępowania z ryzykiem naruszenia ochrony danych osobowych

„Plan postępowania z ryzykiem" opisuje zaplanowane działania postępowania z ryzykiem – minimalizujące ryzyko. „Plan postępowania z ryzykiem" stanowi integralną część „Karty ryzyka". Dla wszystkich aktywów/procesów, których poziom ryzyka będzie „niedopuszczalny", konieczne będzie wdrożenie środków minimalizujących ryzyko poprzez zastosowanie jednej lub kilku strategii opisanych poniżej:

- wdrożenie dodatkowych zabezpieczeń,
- świadome zaakceptowanie przez kierownictwo ryzyka na poziomie przekraczającym próg akceptowalności,
- przeniesienie ryzyka na inny podmiot (np. ubezpieczenia),
- uniknięcie ryzyka (np. zaprzestanie przetwarzania danych osobowych).

Po wdrożeniu środków minimalizujących ryzyko, skuteczność wprowadzonych środków powinno poddać się ocenie. Ocena ta powinna mieć odzwierciedlenie w „Karcie ryzyka". Ze względu fakt, że wprowadzanie środków minimalizujących ryzyko wiążę się z przeznaczeniem zasobów, plan postępowania z ryzykiem wymaga akceptacji Administratora Danych.

6. ZARZĄDZANIE DOKUMENTEM

Dokument wchodzi w życie z dniem podpisania przez Administratora.
Właścicielem tego dokumentu jest Administrator Danych lub osoba przez niego upoważniona.
Dokumentacja zawiera:

- Załącznik nr 1. Wzorcowa lista kontrolna ryzyk;
- Załącznik nr 2. Wzorcowa karta klasyfikacji procesów przetwarzania danych osobowych
- Załącznik nr 3. Wzorcowa karta oceny skutków naruszenia ochrony danych osobowych;
- Załącznik nr 4. Wzorcowy rejestr ryzyk naruszenia ochrony danych osobowych.

Załączniki stanowią integralną część dokumentu – wymagają nadzoru, jednak dokonywane w nich zmiany (zawartość, sposób prezentacji) nie wymagają aktualizacji polityki bezpieczeństwa.

Aktualna wersja oraz data wydania jest wymaganym elementem identyfikacji załącznika.

7. HISTORIA DOKUMENTU.

Data / wydanie	Opis zmiany
20.09.2018 r. / v.1	Utworzenie dokumentu.

Załącznik nr 1 do
Metodyki oceny skutków dla ochrony danych osobowych - wzorcowa lista kontrolna ryzyk

Lista kontrolna ryzyk numer: .....

L.P.	ZAGROŻENIE	ŹRÓDŁA ZAGROŻENIA*	PRAWDO-PODOBIEŃSTWO	WPŁYW	RYZYKO	INFORMACJE NA TEMAT PODATNOŚCI/UWAGI
	ZNISZCZENIA FIZYCZNE					
1.	Pożar	P, U, N	małe	duży	niskie	
2.	Zalanie	P, U, N	małe	duży	niskie	
3.	Zanieczyszczenie	P, U, N	małe	duży	niskie	
4.	Poważny wypadek	P, U, N	małe	duży	niskie	
5.	Zniszczenie urządzeń lub nośników	P, U, N	małe	duży	niskie	
6.	Pył, korozja, wychłodzenie	P, U, N	małe	znaczny	niskie	
	ZJAWISKA NATURALNE					
7.	Zjawiska klimatyczne	N	małe	małe	niskie	
8.	Zjawiska sejsmiczne	N	małe	małe	niskie	
9.	Zjawiska wulkaniczne	N	małe	małe	niskie	
10.	Zjawiska pogodowe	N	małe	małe	niskie	
11.	Powódź	N	małe	małe	niskie	
	UTRATA PODSTAWOWYCH USŁUG					
12.	Awaria systemu klimatyzacji lub dostaw wody	P, U	małe	małe	niskie	
13.	Utrata dostaw prądu	P, U, N	małe	małe	niskie	
14.	Awaria urządzenia telekomunikacyjnego	P, U	małe	znaczny	niskie	
	ZAKŁÓCENIA SPOWODOWANE PROMIENIOWANIEM					
15.	Promieniowanie elektromagnetyczne	P, U, N	małe	małe	niskie	
16.	Promieniowanie cieplne	P, U, N	małe	małe	niskie	
17.	Impuls elektromagnetyczny	P, U, N	małe	małe	niskie	
	AWARIE TECHNICZNE					
18.	Awaria urządzenia	P	małe	małe	niskie	
19.	Niewłaściwe funkcjonowanie urządzeń	P	małe	małe	niskie	
20.	Przeciążenie systemu informacyjnego	P, U	małe	małe	niskie	
21.	Niewłaściwe funkcjonowanie oprogramowania	P	małe	znaczny	niskie	
22.	Naruszenie zdolności utrzymania systemu informacyjnego	P, U	małe	duży	niskie	

L.P.	ZAGROŻENIE	ŹRÓDŁA ZAGROŻENIA*	PRAWDO-PODOBIEŃSTWO	WPŁYW	RYZYKO	INFORMACJE NA TEMAT PODATNOŚCI/UWAGI
	NARUSZENIE BEZPIECZEŃSTWA INFORMACJI					
1.	Przechwycenie sygnałów na skutek zjawiska interferencji	U	małe	znaczny	niskie	
2.	Szpiegostwo zdalne	U	małe	znaczny	niskie	
3.	Podsłuch	U	małe	znaczny	niskie	
4.	Kradzież nośników lub dokumentów	U	małe	znaczny	niskie	
5.	Kradzież urządzenia	U	małe	znaczny	niskie	
6.	Odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników	U	małe	znaczny	niskie	
7.	Ujawnienie	P, U	małe	znaczny	niskie	
8.	Dane z niewiarygodnych źródeł	P, U	małe	znaczny	niskie	
9.	Manipulowanie urządzeniem	U	małe	znaczny	niskie	
10.	Sfałszowanie oprogramowania	P, U	małe	znaczny	niskie	
11.	Detekcja umiejscowienia	U		znaczny	brak	
	NIEAUTORYZOWANE DZIAŁANIA					
1.	Nieautoryzowane użycie urządzeń	U	małe	duży	niskie	
2.	Nieuprawnione kopiowanie oprogramowania	U	małe	duży	niskie	
3.	Użycie fałszywego lub skopiowanego oprogramowania	P, U	małe	duży	niskie	
4.	Zniekształcenie danych	U	małe	znaczny	niskie	
5.	Nielegalne przetwarzanie danych	U	małe	duży	niskie	
6.	Naruszenie bezpieczeństwa funkcji	P, U	małe	duży	niskie	
7.	Błąd użytkowania	P	małe	duży	niskie	
8.	Naruszenie praw	P, U	małe	duży	niskie	
9.	Fałszowanie praw	U	małe	znaczny	niskie	
10.	Odmowa działania	U	małe	niski	niskie	
11.	Naruszenie dostępności personelu	P, U, N	małe	duży	niskie	

* / P- przypadkowe/ U-umyślne/ N-Naturalne

Uwagi: . . brak. . . . . INSPEKTOR OCHRONY DANYCH OSOBOWYCH

. . . . . Data . .16.08.2019r. . . .Przygotował . .IOD-Krzysztof Dybeł. . . .

inż. Krzysztof Dybeł

L.P.	ZAGROŻENIE	ŹRÓDŁA ZAGROŻENIA*	PRAWDO-PODOBIEŃSTWO	WPŁYW	RYZYKO	INFORMACJE NA TEMAT PODATNOŚCI/UWAGI
	NARUSZENIE BEZPIECZEŃSTWA INFORMACJI					
1.	Przechwycenie sygnałów na skutek zjawiska interferencji	U	małe	znaczny	niskie	
2.	Szpiegostwo zdalne	U	małe	znaczny	niskie	
3.	Podsłuch	U	małe	znaczny	niskie	
4.	Kradzież nośników lub dokumentów	U	małe	znaczny	niskie	
5.	Kradzież urządzenia	U	małe	znaczny	niskie	
6.	Odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników	U	małe	znaczny	niskie	
7.	Ujawnienie	P, U	małe	znaczny	niskie	
8.	Dane z niewiarygodnych źródeł	P, U	małe	znaczny	niskie	
9.	Manipulowanie urządzeniem	U	małe	znaczny	niskie	
10.	Sfałszowanie oprogramowania	P, U	małe	znaczny	niskie	
11.	Detekcja umiejscowienia	U		znaczny	brak	
	NIEAUTORYZOWANE DZIAŁANIA					
1.	Nieautoryzowane użycie urządzeń	U	małe	duży	niskie	
2.	Nieuprawnione kopiowanie oprogramowania	U	małe	duży	niskie	
3.	Użycie fałszywego lub skopiowanego oprogramowania	P, U	małe	duży	niskie	
4.	Zniekształcenie danych	U	małe	znaczny	niskie	
5.	Nielegalne przetwarzanie danych	U	małe	duży	niskie	
6.	Naruszenie bezpieczeństwa funkcji	P, U	małe	duży	niskie	
7.	Błąd użytkowania	P	małe	duży	niskie	
8.	Naruszenie praw	P, U	małe	duży	niskie	
9.	Fałszowanie praw	U	małe	znaczny	niskie	
10.	Odmowa działania	U	małe	niski	niskie	
11.	Naruszenie dostępności personelu	P, U, N	małe	duży	niskie	

* / P- przypadkowe/ U-umyślne/ N-Naturalne

Uwagi: . . brak. . . . . .

. . . . . Data . . . . . .Przygotował . . IOD-Krzysztof Dybeł. . . .

Załącznik nr 1 do
Metodyki oceny skutków dla ochrony danych osobowych - wzorcowa lista kontrolna ryzyk

Lista kontrolna ryzyk numer: .....

L.P.	ZAGROŻENIE	ŹRÓDŁA ZAGROŻENIA*	PRAWDO-PODOBIEŃSTWO	WPŁYW	RYZYKO	INFORMACJE NA TEMAT PODATNOŚCI/UWAGI
	ZNISZCZENIA FIZYCZNE					
1.	Pożar	P, U, N	małe	duży	niskie	
2.	Zalanie	P, U, N	małe	duży	niskie	
3.	Zanieczyszczenie	P, U, N	małe	duży	niskie	
4.	Poważny wypadek	P, U, N	małe	duży	niskie	
5.	Zniszczenie urządzeń lub nośników	P, U, N	małe	duży	niskie	
6.	Pył, korozja, wychłodzenie	P, U, N	małe	znaczny	niskie	
	ZJAWISKA NATURALNE					
7.	Zjawiska klimatyczne	N	małe	małe	niskie	
8.	Zjawiska sejsmiczne	N	małe	małe	niskie	
9.	Zjawiska wulkaniczne	N	małe	małe	niskie	
10.	Zjawiska pogodowe	N	małe	małe	niskie	
11.	Powódź	N	małe	małe	niskie	
	UTRATA PODSTAWOWYCH USŁUG					
12.	Awaria systemu klimatyzacji lub dostaw wody	P, U	małe	małe	niskie	
13.	Utrata dostaw prądu	P, U, N	małe	małe	niskie	
14.	Awaria urządzenia telekomunikacyjnego	P, U	małe	znaczny	niskie	
	ZAKŁÓCENIA SPOWODOWANE PROMIENIOWANIEM					
15.	Promieniowanie elektromagnetyczne	P, U, N	małe	małe	niskie	
16.	Promieniowanie cieplne	P, U, N	małe	małe	niskie	
17.	Impuls elektromagnetyczny	P, U, N	małe	małe	niskie	
	AWARIE TECHNICZNE					
18.	Awaria urządzenia	P	małe	małe	niskie	
19.	Niewłaściwe funkcjonowanie urządzeń	P	małe	małe	niskie	
20.	Przeciążenie systemu informacyjnego	P, U	małe	małe	niskie	
21.	Niewłaściwe funkcjonowanie oprogramowania	P	małe	znaczny	niskie	
22.	Naruszenie zdolności utrzymania systemu informacyjnego	P, U	małe	duży	niskie	

Załącznik nr 4 do
Metodyki oceny skutków dla ochrony danych osobowych
Wzorcowy rejestr ryzyk naruszenia ochrony danych osobowych

Lp.	Data oceny	Numer karty ryzyka	Zidentyfikowane ryzyka - niedopuszczalne	Data zakończenia działań
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

Załącznik nr 2 do
Metodyki oceny skutków dla ochrony danych osobowych
Wzorcowa karta klasyfikacji procesów przetwarzania danych osobowych

Lp.	Obszar podlegający klasyfikacji :	Dane osobowe	Właściciel zasobu - gestor	P[1]	D[2]	I[3]
1	Zasób informacyjny/proces :					
2	Zasób informacyjny/proces :					
3	Zasób informacyjny/proces :					
4	Zasób informacyjny/proces :					
5	Zasób informacyjny/proces :					
6	Zasób informacyjny/proces :					
7	Zasób informacyjny/proces :					
8	Wymagania odnośnie bezpieczeństwa:					

Data sporządzenia: ..... Sporządził(a): .....

P[1]-Poufność, D[2]-Dostępność, I[3]-Integralność