CENTRUM KULTURALNE
ul. S. Konarskiego 9
37-700 Przemyśl
tel./fax 16 678-20-09
NIP 795-21-24-902, Regon 650953538

Analiza ryzyka w procesie obsługi sygnalistów

Obsługa zgłoszeń sygnalistów									
1	2	3	4	5	6	7	8	9	10
Zidentyfikowane zagrożenie	Możliwy skutek zmaterializowania się zagrożenia	Zagrożony atrybut: poufność/integralność/ dostępność	Istotność zagrożenia	Wartość poziomu istotności	Prawdopodobieństwo wystąpienia zagrożenia	Wartość prawdopodobieństwa	Potencjalne ryzyko	Proponowane zabezpieczenia do wdrożenia	Prawdopodobny skutek wdrożenia działań zabezpieczających
Przechowywanie na nośniku (np.. pendrive) prywatnym/niezabezpieczonym dokumentacji zgłoszeń	Zgubienie lub kradzież nośnika	poufność	Poziom bardzo wysoki	5	wysokie	4	20	wprowadzić regulacje dotyczące sposobu postępowania z nośnikami, podmiot prawny powinien wprowadzić zakaz przechowywania dokumentacji na nośniku lub ograniczyć wyłącznie do służbowych zabezpieczonych nośników	zmniejszenie ryzyka
Pozostawienie dokumentacji zgłoszenia(forma papierowa lub wydruk) w miejscu dostępnym dla osób postronnych	Osoby nieupoważnione uzyskają dostęp do danych sygnalisty i osób wskazanych w zgłoszeniu	poufność; ryzyko zagrożenia dostępności, jeżeli zgłoszenie wpłynęło w formie papierowej	Poziom bardzo wysoki: może doprowadzić do dyskryminowania sygnalisty	5	średnie: możliwe wystąpienie błędu ludzkiego	3	15	działanie uświadamiające: szkolenia i przypominanie zasad postępowania z dokumentacją zawierającą dane osobowe	zmniejszenie ryzyka
Przekroczenie czasu przechowywania dokumentacji przez przedmiot zewnętrzny	przechowywanie niezgodne z prawem	poufność	Poziom średnio wysoki: dłuższe przechowywanie dokumentacji zgłoszeń wywołuje ryzyka np.. przy przypadkowym ujawnieniu dokumentacji	5	niskie: czas przechowywania określony jest przepisami prawa	2	10	cykliczne sprawdzanie podmiotu przetwarzającego i sposobu przetwarzania	ograniczenie ryzyka pomijalnego
Brak weryfikacji podmiotu zewnętrznego przez podmiot prawny	wyciek danych, ujawnienie danych osobom nieuprawnionym, wystąpienie naruszenia ochrony danych	poufność, dostępność	Poziom wysoki przy zupełnym braku weryfikacji	5	wysokie przy braku weryfikacji	5	25	wdrożenie procedury weryfikacji podmiotu przetwarzającego przed zawarciem umowy powierzenia	zmniejszenie ryzyka
Ujawnienie danych sygnalisty bez jego zgody	Dostęp osób nieuprawnionych do danych sygnalisty, naruszenie przepisów ustawy o ochronie sygnalistów	poufność	Poziom bardzo wysoki: naruszenie przepisów ustawy może także wywołać szkody wizerunkowe dla administratora	5	niskie przy wdrożonej procedurze	3	10	wdrożyć procedurę pozyskiwania zgody sygnalisty	ograniczenie ryzyka pomijalnego
Pozostawienie danych niepotrzebnych w zgłoszeniu	naruszenie zasady ograniczenia przechowywania i minimalizacji	poufność	Poziom wysoki z uwagi na skutki naruszenia przepisów ustawy	5	średnie – pracodawca stosuje przepisy ustawy i nadzoruje ich stosowanie	3	15	wdrożyć i stosować procedurę retencji	zmniejszenie ryzyka
Pożar	utrata dokumentacji zgłoszeń sygnalistów, rejestru zgłoszeń	poufność, dostępność	poziom bardzo wysoki: możliwa utrata dokumentacji	5	niskie: pomieszczenie wyposażone w czujniki dymu i alarmy przeciwpożarowe	2	10	zweryfikować stan i sprawność zabezpieczeń przeciwpożarowych	ograniczenie ryzyka pomijalnego

Prawdopodobieństwo wystąpienia zagrożenia					
	Pomijalne	Niskie	Średnie	Wysokie	Bardzo wysoki – krytyczne
Istotność zagrożenia	1	2	3	4	5
pomijalna 1	1	2	3	4	5
niska 2	2	4	6	8	10
średnia 3	3	6	9	12	15
wysoka 4	4	8	12	16	20
Bardzo wysoka – krytyczna (5)	5	10	15	20	25
Ryzyko – stopień	pomijalne 1-7	niskie 8-14	średnie 15-25	wysokie 15-25	

p.o. DYREKTOR


Janusz Czarski