PROCEDURA ZASADY POSTĘPOWANIA W PRZYPADKU INCYDENTU NARUSZENIA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

	Stanowisko:	Imię i nazwisko:	Data:	Podpis:
Opracował	Inspektor Ochrony Danych Osobowych	Jacek Gołdych	15. CZE. 2021	INSPEKTOR Ochrony Danych Osobowych Jacek Gołdych
Zatwierdził pod względem formalno – prawnym	Dyrektor WSZZOZ	Sławomir Wysocki	15. CZE. 2021	Wojewódzkiego Specjalistycznego ZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza lek. med. Sławomir Wysocki

1. Cel:

Wdrożenie zasad postępowania w przypadku incydentu naruszenia bezpieczeństwa przetwarzania danych osobowych.

2. Zakres stosowania:

2.1. Postanowienia zawarte w niniejszej procedurze obowiązują w WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza.

3. Odpowiedzialność:

3.1 Administrator Danych Osobowych odpowiada za:

- Podejmowanie decyzji dotyczących zasad postępowania w przypadku wystąpienia incydentu naruszenia bezpieczeństwa danych osobowych,
- Nadzór i koordynację działań związanych z podjęciem działań w ramach analizy przyczyny wystąpienia incydentu jako i wszelkich działań z nim związanych dla zminimalizowania skutków incydentu.

3.2. Inspektor Ochrony Danych Osobowych odpowiada za:

- Analizę przedmiotu i okoliczności wystąpienia incydentu,
- Analizę i identyfikację przyczyny zaistnienia incydentu,
- Wskazywanie sposobów i kierunków działania na rzecz minimalizacji skutków zaistniałego zdarzenia,
- Sporządzanie dokumentacji w ramach zidentyfikowanego incydentu i jej archiwizację/ zabezpieczanie,
- Sporządzanie dokumentacji do Organu Nadzorczego zgodnie z przepisami prawa.

3.3. Pracownicy WSZZOZ odpowiadają za:

- Reagowanie na wszelkie zauważone nieprawidłowości w procesie przetwarzania danych osobowych mogących sugerować wystąpienie incydentu naruszenia bezpieczeństwa danych osobowych i niezwłoczne zgłoszenie zdarzenia do Administratora Danych Osobowych opcjonalnie Inspektora Ochrony Danych Osobowych.

4. Terminologia

Incydent związany z bezpieczeństwem informacji- to pojedyncze zdarzenie lub seria zdarzeń niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji, w tym danych osobowych.

Zdarzenie będące potencjalnie incydentem – zdarzenie związane z wystąpieniem sytuacji podczas, której nie dochodzi do zaistnienia incydentu jednak towarzyszące jej okoliczności, mogą do takiego incydentu doprowadzić.

5. Tryb postępowania

5.1. Każdy z pracowników z osób współpracujących z WSZZOZ Chorób Płuc i Gruźlicy w Wolicy k/Kalisza każdorazowo w sytuacji zidentyfikowania zdarzenia/okoliczności co do których istnieje

prawdopodobieństwo, że informacja/dane będące własnością/w posiadaniu WSZZOZ mogły być w jakikolwiek sposób narażone na nieuprawnione wykorzystanie lub narażone na utratę ich poufności, integralności czy dostępności zobowiązany jest niezwłocznie po zidentyfikowaniu zdarzenia zgłosić je do Dyrektora WSZZOZ opcjonalnie Inspektora Ochrony Danych osobowych.

5.2. Osoba zgłaszająca zdarzenie odpowiada za wyczerpujące opisanie incydentu adekwatnie do posiadanej wiedzy i umiejętności.

5.3. Brak tej wiedzy i umiejętności poprawnego rozpoznania, a także klasyfikacji typu oraz poziomu istotności incydentu po stronie osoby zgłaszającej nie może być przyczyną zaniechania zgłoszenia incydentu.

5.4. Zgłoszony incydent należy właściwie zapisać – karta zgłoszenia incydentu.

5.5. Osobą odpowiedzialną za wstępną analizę zgorszonych incydentów jest Inspektor Ochrony Danych Osobowych opcjonalnie we współpracy ze Specjalistą ds. IT,

5.6. Zgłoszony incydent podlega weryfikacji i jednoznacznemu zdefiniowaniu czy w wyniku zdarzenia doszło lub mogło dojść do utraty poufności, integralności i dostępności informacji jak również skutków zaistniałego zdarzenia.

5.7. W przypadku, gdy zgłoszone zdarzenie po przeprowadzonej wstępnej analizie uznane zostało jako nieistotne w aspekcie bezpieczeństwa informacji = tym samym nie jest incydentem Inspektor Ochrony Danych Osobowych zobowiązany jest poinformować o tym fakcie osobę zgłaszającą (e-mail),

5.8. Na etapie prowadzonej analizy wstępnej zaistniałego zdarzenia, osoba odpowiedzialna za obszar, w którym doszło do potencjalnego incydentu i/lub osoba identyfikująca zdarzenie odpowiedzialna jest za takie zabezpieczenie danych/informacji, aby nie utraciły one atrybutów dostępności, integralności, poufności i autentyczności,

5.9. Na podstawie zgromadzonych informacji incydent jest oceniany pod kątem krytyczności i rozmiaru wpływu na WSZZOZ bądź jej poszczególne procesy biznesowe,

5.10. Krytycznymi incydentami są incydenty bezpieczeństwa informacji, które dotykają infrastruktury teleinformatycznej i systemów, od których zależy ciągłość działania lub których skutkiem mogą być znaczne straty finansowe czy też poważny uszczerbek na reputacji, poufności danych osobowych itp. Kierując się wrażliwością danych oraz skalą skutków incydentu, należy ocenić poziom jego istotności. Z chwilą ich zidentyfikowania w proces wstępnej analizy niezwłocznie włączany jest Specjalista ds. IT (zewnętrzna firma),

5.11. Po rozpoznaniu incydentu bezpieczeństwa i pozyskaniu na jego temat niezbędnych danych, podejmowane są przez Administratora Danych Osobowych we współpracy z Inspektorem Ochrony Danych Osobowych i Specjalistą ds. IT, działania mające na celu powstrzymanie dalszego przebiegu incydentu, ograniczenie zasięgu oraz szkodliwości jego skutków dla Zakładu.

5.12. Postępowanie naprawcze polega na wdrożeniu działań, mających na celu przywrócenie ciągłości operacyjnej, odzyskanie danych, przywrócenie pełnej funkcjonalności oraz zapewnienie bezpieczeństwa systemów i procesów, usunięcie z systemów śladów incydentów (usuniecie szkodliwego oprogramowania, odblokowanie kont użytkowników zablokowanych wskutek wystąpienia incydentu itp.), a także przeciwdziałanie podobnym incydentom w przyszłości,

5.13. Wszystkie podejmowane działania należy na bieżąco dokumentować. Najważniejsze to:

a) całość pozyskanego materiału w zakresie zgłoszonego incydentu (miejsce, czas, sytuacja w jakiej zidentyfikowano zdarzenie, inne towarzyszące kwestie mające związek z incydentem)
b) wprowadzone zmiany w systemach i procesach;
c) potencjalne straty i szkody związane z incydentem.

5.14 W przypadku incydentu, co do którego istnieje prawdopodobieństwo, iż jego wystąpienie dotyczy danych osobowych Inspektor Ochrony Danych Osobowych zobowiązany jest w procesie analizy

szczegółowo zweryfikować skutek zaistniałego zadaszenia dla osoby fizycznej/osób których dane dotyczą. Weryfikacja powinna uwzględniać, czy zdarzanie nie może potencjalnie skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych osób fizycznych, których dane dotyczą.

5.15. Zgromadzona i odpowiednio zabezpieczona dokumentacja z postępowania z incydentami bezpieczeństwa musi być przechowywana przez okres co najmniej trzech lat z wyjątkiem sytuacji, wymagany ogólnie obowiązującymi przepisami prawa.

5.16. W przypadku analizy incydentu w bezpieczeństwie informacji, którego skutek dotyczył przetwarzanych danych osobowych/osoby fizycznej Inspektor Ochrony Danych Osobowych zobowiązany jest do zgłoszenia zdarzenia odpowiednim organom zgodnie z wymaganiami prawnymi w zakresie ochrony danych osobowych, za wyjątkiem sytuacji kiedy WSZZOZ jest w stanie wykazać zgodnie z zasada rozliczalności, że jest mało prawdopodobne, by naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.

5.17. W przypadku, kiedy analiza incydentu w bezpieczeństwie informacji jednoznacznie wskazuje na naruszenie przez pracownika/osobę współpracującą z WSZZOZ zasad polityki bezpieczeństwa informacji Dyrektora WSZZOZ podejmuje decyzję co do dalszej współpracy.

6. Załączniki

6.1. Wzór formularza zgłoszenia incydentu naruszenia bezpieczeństwa danych osobowych.