Procedura postępowania w sytuacji naruszenia ochrony danych osobowych w Globomed sp. z o.o. z siedzibą w Białymstoku wpisaną do rejestru podmiotów wykonujących działalność leczniczą prowadzonego przez Wojewodę Podlaskiego pod nazwą „Właśnie Tu"

1. Definicje związane z naruszeniem bezpieczeństwa danych osobowych

1.1. Co to jest incydent?

Incydent to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Jest to sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

1.2. Przykłady naruszeń bezpieczeństwa

Naruszenie	Skutek	Opis
1) Nadanie zbyt wysokich uprawnień użytkownikom. 2) Brak kontroli nad dostępem do plików, baz, komputerów, dokumentów papierowych. 3) Udostępnienie niezabezpieczonych kopii zapasowych danych w sieci. 4) Instalacja programów szpiegujących. 5) Ujawnienie danych dostępowych do systemów IT w wyniku ataku socjotechnicznego. 6) Kradzież lub zgubienie sprzętu lub nośnika z danymi. 7) Upublicznienie danych w przestrzeni publicznej, dostęp przez Internet, przesłanie lub wydawanie informacji osobie nieupoważnionej, wyrzucanie na śmietnik uszkodzonych nośników bez ich zniszczenia. 8) Naruszenie pisemnych lub ustnych procedur, np. niewylogowanie się z systemu, przekazanie haseł koledze, przechowywanie zapisanych loginów i haseł w pobliżu komputera. 9) Kopiowanie danych z katalogów, dysków, baz, programów, kserowanie i robienie zdjęć przez nieupoważnionego pracownika lub przez osobę obcą.	Nieuprawniony dostęp do danych	Kradzież tożsamości – np. przejęcie poczty elektronicznej, dostępu do bazy danych, plików czy dokumentów papierowych. Ujawnienie tych danych lub ich wykorzystanie w zakresie szkodzącym firmie.
1) Awaria sprzętu i oprogramowania w skutek nieprawidłowego administrowania (np. brak aktualizacji i sterowników, brak UPS-ów, niewystarczająca wiedza w zakresie IT). Brak procedur w zakresie ciągłości działania.	Brak dostępu do zasobów z danymi osobowymi	Brak możliwości: - przetwarzania danych; - realizowania żądań strony w zakresie jej praw;
2) Pomyłka pracownika przy wprowadzaniu/modyfikowaniu danych. Nieumiejętne administrowanie bazą danych lub serwerem plików. Celowe działanie pracownika lub osoby z zewnątrz skutkujące modyfikacją lub usunięciem danych – ataki hakerskie, cyberterroryzm.	Nieuprawniona modyfikacja / usunięcie danych	Nieprzeszkolony personel. Niezadowolony pracownik lub osoba z zewnątrz o złych zamiarach – ataki hakerskie, cyberterroryzm.

1.3. Sytuacje wskazujące na możliwość wystąpienia incydentu

1. ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
2. fizyczna obecność w budynku osób zachowujących się podejrzanie,

3. niezabezpieczone pomieszczenia, meble, urządzenia, nośniki danych, gdzie przetwarzane są dane osobowe (np. pozostawienie otwartych drzwi, szaf i niewylogowanego komputera bez nadzoru, pozostawienie wydruków z danymi na ogólnodostępnej drukarce),
4. niszczenie dokumentacji papierowej zawierającej dane osobowe bez użycia niszczarki,
5. nieprawidłowe ustawienie monitorów, które pozwala na podgląd przez osoby postronne oraz przechowywanie zapisanych loginów i haseł dostępu do systemów IT w pobliżu komputera,
6. wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia,
7. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej,
8. wykrycie próby modyfikacji danych lub zmiany w strukturze danych bez autoryzacji,
9. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
10. telefoniczne i e-mailowe próby wyłudzenia danych osobowych, loginów i haseł dostępu do systemów IT (ataki socjotechniczne),
11. kradzież lub zagubienie komputerów/ urządzeń przenośnych/ nośników danych zawierających dane osobowe,
12. wykrycie nieautoryzowanych kont dostępu do danych lub tzw. „Backdoor",
13. utrata kontroli nad kopią danych osobowych.

2. Sposób postępowania w przypadku podejrzenia naruszenia danych osobowych

1. Każdy pracownik, który podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to Administratorowi Danych Osobowych reprezentowanemu przez członków zarządu Globomed sp. z o.o.
2. W przypadku stwierdzenia podejrzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia. Nie należy opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia osoby upoważnionej przez Administratora Danych Osobowych.
3. Administrator Systemu Informatycznego jest zobowiązany do informowania osoby wyznaczonej przez Administratora Danych Osobowych o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.
4. Osoba wyznaczona przez Administratora Danych Osobowych podejmuje następujące kroki:
   a) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
   b) spisuje w postaci notatki służbowej relację od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać istotne informacje w sprawie (pkt. 5),
   c) ściśle współpracuje ze specjalistami w zakresie IT (administrator systemu informatycznego, sieci komputerowej, bazy danych itp.),
   d) dokonuje analizy czy jest to incydent w rozumieniu przepisów RODO i informuje Administratora Danych Osobowych o wynikach tej analizy.

5. Administrator Danych Osobowych na podstawie analizy przekazanej przez osobę przez niego wyznaczoną podejmuje decyzję o uznaniu lub nie zdarzenia za incydent w rozumieniu przepisów RODO.

3. Sposób postępowania w przypadku naruszenia danych osobowych

1. W przypadku naruszenia ochrony danych osobowych, Administrator Danych Osobowych bez zbędnej zwłoki w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je Prezesowi Urzędu Ochrony Danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi

nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. (Procedura zgłoszenia naruszenia danych osobowych – pkt. 6).

2. Zgłoszenie, o którym mowa powyżej, musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Jeżeli informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

4. Administrator Danych Osobowych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

5. Administrator Danych Osobowych prowadzi w formie elektronicznej Rejestr naruszeń (pkt. 7).

6. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

7. Zawiadomienie jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera:

a) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
b) opis możliwych konsekwencji naruszenia ochrony danych osobowych,
c) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

8. Zawiadomienie, o którym mowa powyżej, nie jest wymagane, w następujących przypadkach:

a. administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
b. wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

4. Odpowiedzialność w związku z niepodjęciem działań w przypadku zaobserwowania potencjalnego naruszenia danych osobowych

Wobec osoby, która w przypadku zaobserwowania potencjalnego naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych/współpracy. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o potencjalnym naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym

przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę/ Zlecającego o zrekompensowanie poniesionych strat.

5. Wzór notatki z naruszeniem danych osobowych

Notatka z incydentu naruszenia ochrony danych w Globomed sp. z o.o. z siedzibą w Białymstoku,
wpisanej do rejestru podmiotów wykonujących działalność leczniczą prowadzonego przez Wojewodę Podlaskiego pod nazwą „Właśnie Tu"

Data: ..... godzina otrzymania zgłoszenia: .....

Osoba przekazująca informację o potencjalnym naruszeniu (imię, nazwisko, stanowisko służbowe):
.....

Inne osoby zaangażowane lub odpytane w związku ze zgłoszonym zdarzeniem (imię, nazwisko, stanowisko służbowe):
.....

Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, identyfikator stanowiska komputerowego, nazwa systemu lub aplikacji itp.):
.....
.....

Rodzaj potencjalnego naruszenia i określenie okoliczności towarzyszących zdarzeniu:
.....
.....

Podjęte działania:
.....
.....

Podjęte działania ze strony Administratora Danych Osobowych:
.....
.....

Wstępna ocena przyczyn wystąpienia potencjalnego naruszenia:
.....
.....

.....
(podpis osoby sporządzającej notatkę)

Zapoznałem się
.....
(podpis Administratora Danych Osobowych)

6. Procedura zgłoszenia naruszenia danych osobowych

1. W celu zgłoszenia naruszenia ochrony danych osobowych należy pobrać i wypełnić „Zgłoszenie naruszenia danych osobowych" ze strony https://uodo.gov.pl/pl/134/233.
2. Wypełnione zgłoszenie można przekazać do Prezesa Urzędu Ochrony Danych Osobowych jako załącznik do **pisma ogólnego dostępnego na platformie biznes.gov.pl** bądź wysłać przez ePUAP na adres elektronicznej skrzynki podawczej: **/GIODO/SkrytkaESP.**
3. Zgłoszenia dokonuje Administrator Danych Osobowych, który w tym celu musi posiadać potwierdzony Profil Zaufany bądź podpis kwalifikowany.

7. Wzór rejestru naruszeń

Strona lewa

Numer naruszenia	Data zgłoszenia naruszenia	Godzina zgłoszenia naruszenia	Osoba zgłaszająca naruszenie	Miejsce naruszenia	System informatyczny	Data naruszenia	Godzina naruszenia

Strona prawa

Krótki opis naruszenia	Osoby uczestniczące w naruszeniu	Skutki naruszenia	Podjęte czynności	Czy zawiadomiono PUOD	Czy zawiadomiono osobę, której dane dotyczą