**Procedura postępowania z naruszeniem ochrony danych osobowych**

§ 1  
**Przedmiot Procedury**

Niniejsza Procedura zawiera szczegółowe rozwiązania względem Rozdziału XV Polityki ochrony danych osobowych „Naruszenia Bezpieczeństwa Danych Osobowych”, stosownie do 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, dalej „**RODO**”).

§ 2  
**Definicja Administratora danych osobowych i naruszenia ochrony danych osobowych**

1. Administratorem danych osobowych jest Uniwersytet Medyczny im. Piastów Śląskich we Wrocławiu, z siedzibą przy Wybrzeżu L. Pasteura 1, 50-367 Wrocław, reprezentowany przez Rektora („**Administrator**”).
2. Naruszeniem ochrony danych osobowych jest każde zdarzenie, powodujące zagrożenie bezpieczeństwa danych osobowych, w szczególności:   
   2.1. prowadzące do utraty integralności danych (np. pozostawianie dokumentów   
    zawierających dane w miejscach powszechnie dostępnych),  
   2.2. zagrażające poufności danych (np. przesyłanie danych drogą elektroniczną bez   
    zabezpieczenia dostępu do plików),  
   2.3. zagrażające dostępności do danych (np. zgubienie nośnika pendrive, na którym   
    znajdowały się dane osobowe, a użytkownik nośnika nie sporządził kopii zapasowej),  
   2.4. zagrażające rozliczalności danych (np. korzystanie przez kilka osób z jednego hasła   
    dostępu).
3. Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:   
   3.1. stwierdzono naruszenie obowiązujących przepisów wewnętrznych,   
   3.2. stwierdzono naruszenie powszechnie obowiązujących przepisów prawa,   
   3.3. stwierdzono naruszenie zabezpieczeń fizycznych lub informatycznych,   
   3.4. stan sprzętu komputerowego, zawartość zbioru danych osobowych, ujawnione metody   
    pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej   
    mogą wskazywać na naruszenie zabezpieczeń tych danych,   
   3.5. inne okoliczności wskazujące, że mogło nastąpić nieuprawnione udostępnienie danych   
    osobowych przetwarzanych przez Administratora.
4. Przykładowy katalog naruszeń zagrażających bezpieczeństwu danych osobowych zawiera Załącznik nr 1 do niniejszej Procedury.

§ 3  
**Postępowanie pracownika lub innej osoby przetwarzającej dane w przypadku podejrzenia naruszenia ochrony danych osobowych**

1. O każdym przypadku podejrzenia naruszenia ochrony danych osobowych należy powiadomić przełożonego, Inspektora Ochrony Danych, a w przypadku, gdy naruszenie dotyczy systemu informatycznego, także Centrum Informatyczne.
2. Sposób powiadomienia:  
   2.1. pracownik, inna osoba przetwarzająca dane osobowe lub ich przełożony wypełnia   
    formularz „Zawiadomienie o naruszeniu ochrony danych osobowych”, stanowiący   
    Załącznik nr 2 do niniejszej Procedury,  
   2.2. wypełniony formularz należy przesłać Inspektorowi Ochrony Danych,   
    wyłącznie w formie elektronicznej, poprzez system EZD.
3. Powiadomienia należy dokonać niezwłocznie, jednak nie później niż w ciągu 24 godzin od stwierdzenia podejrzenia naruszenia ochrony danych osobowych.
4. W przypadku jakichkolwiek wątpliwości pracownik powinien skonsultować się z Inspektorem Ochrony Danych, np. w kwestii poprawnego wypełnienia formularza.
5. Każda osoba, która stwierdzi podejrzenie naruszenia ochrony danych jest zobowiązana w miarę możliwości podjąć czynności niezbędne do powstrzymania skutków naruszenia.

 § 4  
**Postępowanie Centrum Informatycznego**

W przypadku, gdy naruszenie ochrony danych osobowych dotyczy systemów informatycznych, Centrum Informatyczne współpracuje z Inspektorem Ochrony Danych w celu ustalenia przyczyn, charakteru i okoliczności naruszenia, a także:

* 1. podejmuje działania mające na celu ograniczenie negatywnych skutków naruszenia,
  2. rekomenduje działania zaradcze w celu zminimalizowania ryzyka wystąpienia podobnych incydentów i zwiększenia bezpieczeństwa systemów informatycznych.

§ 5  
**Postępowanie Inspektora Ochrony Danych**

1. Ocena, czy podejrzenie naruszenia stanowi naruszenie ochrony danych osobowych.  
1.1. Po uzyskaniu informacji o podejrzeniu naruszenia ochrony danych, należy ocenić, czy   
 naruszenie to stanowi naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt   
 12 RODO, a więc czy jest to naruszenie bezpieczeństwa prowadzące do przypadkowego   
 lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego   
 ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych,   
 przechowywanych lub w inny sposób przetwarzanych.

1.2. Jeżeli zgłoszone podejrzenie naruszenia nie stanowi naruszenia ochrony danych osobowych w rozumieniu w art. 4 pkt 12 RODO, wówczas na Administratorze nie ciąży obowiązek zgłoszenia tego faktu organowi nadzorczemu, o czym Inspektor Ochrony Danych niezwłocznie zawiadamia Administratora (władze rektorskie i administracyjne Uniwersytetu).

1.3. W przypadku stwierdzenia innego rodzaju naruszeń przepisów o ochronie danych (np. naruszenia zasad, obowiązków informacyjnych itp.), Administrator nie ma obowiązku zawiadomienia organu nadzorczego. Inspektor Ochrony Danych udziela odpowiednich zaleceń w zakresie obowiązków spoczywających na Administratorze na mocy obowiązujących przepisów.

2. Ocena, czy naruszenie ochrony danych skutkuje ryzykiem naruszenia praw lub wolności osoby, której dane dotyczą i udokumentowanie naruszenia.

2.1. W przypadku stwierdzenia, że nastąpiło naruszenie ochrony danych (incydent bezpieczeństwa pociągający za sobą skutek w postaci zniszczenia, utraty, nieuprawnionego zmodyfikowania, ujawnienia lub dostępu do danych), należy – zgodnie z art. 33 ust. 1 RODO – dokonać oceny prawdopodobieństwa, czy naruszenie ochrony danych skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych.

2.2. W przypadku, gdy:  
2.2.1. naruszenie nie powoduje ryzyka naruszenia praw lub wolności osób fizycznych   
 lub jest ono mało prawdopodobne – Inspektor Ochrony Danych dokonuje wpisu   
 do rejestru incydentów, o czym niezwłocznie informuje Administratora (władze   
 rektorskie i administracyjne Uniwersytetu);   
2.2.2 naruszenie ochrony danych będzie skutkowało ryzykiem naruszenia praw lub   
 wolności osób fizycznych – Inspektor Ochrony Danych dokonuje wpisu do   
 rejestru incydentów oraz rekomenduje Administratorowi (władzom rektorskim i   
 administracyjnym Uniwersytetu) zgłoszenie naruszenia Prezesowi Urzędu   
 Ochrony Danych Osobowych w trybie i na zasadach określonych w art. 33   
 RODO;  
2.2.3 naruszenie ochrony danych osobowych może spowodować wysokie ryzyko   
 naruszenia praw i wolności osób fizycznych – Inspektor Ochrony Danych   
 dokonuje wpisu do rejestru incydentów oraz rekomenduje Administratorowi   
 (władzom rektorskim i administracyjnym Uniwersytetu) zgłoszenie naruszenia   
 organowi nadzorczemu, tj. Prezesowi Urzędu Ochrony Danych Osobowych, w   
 trybie i na zasadach określonych w art. 33 RODO, a także zawiadomienie osób,   
 których dane dotyczą w trybie i na zasadach określonych w art. 34 RODO.

2.3. Wszelkich rekomendacji, o których mowa w pkt 2.2., Inspektor Ochrony Danych dokonuje niezwłocznie, jednak nie później niż w terminie 36 godzin od uzyskania informacji o podejrzeniu naruszenia ochrony danych.

2.4. Treść zawiadomień, o których mowa w pkt. 2.2. przygotowuje Inspektor Ochrony Danych.

2.5. Zawiadomienia osób, o którym mowa w pkt 2.2.3 dokonuje Inspektor Ochrony Danych na podstawie pełnomocnictwa udzielonego przez Administratora.

2.6. Zawiadomienie osób, których naruszenie dotyczy nie jest wymagane w następujących przypadkach:

2.6.1. odnośnie danych, których dotyczy naruszenie wdrożono odpowiednie techniczne i organizacyjne środki ochrony, w szczególności takie jak szyfrowanie uniemożliwiające odczyt danych osobom nieuprawnionym,

2.6.2. zastosowano następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

2.6.3. 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.

§ 6  
**Postępowanie Administratora Ochrony Danych**

1. Zgodnie z art. 33 ust. 3 RODO, Rektor Uniwersytetu zgłasza zaistniałe naruszenie   
 organowi nadzorczemu, tj. Prezesowi Urzędu Ochrony Danych Osobowych, bez zbędnej   
 zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu   
 naruszenia.

2. Dopuszczalne jest późniejsze zawiadomienie, po upływie 72-godzinnego terminu,   
 zwłaszcza w przypadku, gdy naruszenie ma poważny charakter i Administrator   
 koncentruje się w pierwszej kolejności na ograniczeniu skutków naruszenia, a następnie   
 stara się spełnić pozostałe obowiązki, jednak wówczas należy wyjaśnić przyczyny   
 opóźnienia.

3. W przypadku, gdy zgłoszenie wszystkich wymaganych informacji nie jest możliwe z   
 zachowaniem terminu wskazanego w ust. 1, Rektor Uniwersytetu dokonuje zgłoszenia   
 częściowego, tj. przekazuje informacje, które są znane Administratorowi w chwili   
 dokonania zgłoszenia przed upływem 72 godzin, a następnie sukcesywnego uzupełniania   
 zgłoszenie, zgodnie z art. 33 ust. 4 RODO.

§ 7  
**Załączniki do Procedury**

Załącznik nr 1 – Przykładowy katalog naruszeń zagrażających bezpieczeństwu danych osobowych,

Załącznik nr 2 – Formularz „Zawiadomienie o naruszeniu ochrony danych osobowych”.