**Procedura postępowania z naruszeniem ochrony danych osobowych**

Wprowadzenie

§ 1

1. Prawidłowe stosowanie procedury postępowania z naruszeniem ochrony danych osobowych wymaga znajomości obowiązującej Polityki Ochrony Danych Osobowych, w szczególności zawartych w niej wyrażeń takich jak np. Administrator Danych Osobowych oraz zrozumienia zasad przetwarzania danych osobowych.
2. Procedura postępowania z naruszeniem ochrony danych osobowych 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 osobowych, dalej RODO).

Definicja naruszenia

§ 2

1. Naruszeniem ochrony danych osobowych jest każde zdarzenie, zależne jak i niezależne od woli ludzkiej, powodujące zagrożenie bezpieczeństwa danych osobowych, w szczególności :

- prowadzące do utraty integralności danych (np. pozostawianie dokumentów zawierających dane w miejscach powszechnie dostępnych)

- zagrażające poufności danych (np. przesyłanie danych drogą elektroniczną bez zabezpieczenia dostępu do plików)

- zagrażające rozliczalności danych (np. korzystanie przez kilka osób z jednego hasła dostępu)

- zagrażające dostępności do danych (np. zgubienie nośnika pendrive, na którym znajdowały się dane osobowe, a użytkownik nośnika nie sporządził kopii zapasowej).

2. Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:

- stwierdzono naruszenie obowiązujących przepisów wewnętrznych,

- stwierdzono naruszenie obowiązujących przepisów prawa,

- stwierdzono naruszenie zabezpieczeń fizycznych lub informatycznych,

- 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,

- inne okoliczności wskazujące, że mogło nastąpić nieuprawnione udostępnienie danych osobowych przetwarzanych przez jednostkę.

3. Przykładowy katalog naruszeń i incydentów zagrażających bezpieczeństwu danych osobowych zawiera Załącznik nr 1 do niniejszej procedury postępowania.

§ 3

Uzyskanie informacji o podejrzeniu naruszenia ochrony danych osobowych

1. Administrator może uzyskać informacje o naruszeniu przepisów o ochronie danych z różnych źródeł, w szczególności poprzez poinformowanie o tym przez osobę zatrudnioną przy przetwarzaniu danych oraz uzyskanie informacji od podmiotu przetwarzającego dane, który na mocy art. 33 ust. 2  RODO, ma obowiązek bez zbędnej zwłoki zgłosić naruszenie administratorowi.
2. Zgłoszenie podmiotu przetwarzającego odbywa się na zasadach określonych w odrębnych umowach powierzenia przetwarzania danych.

§ 4

Postępowanie pracownika w przypadku stwierdzenia podejrzenia naruszenia ochrony danych osobowych

1. O każdym przypadku podejrzenia naruszenia ochrony danych osobowych należy powiadomić przełożonego oraz inspektora ochrony danych.
2. Forma powiadomienia:
3. Pracownik lub jego przełożony wypełnia formularz „Informacja o naruszeniu – źródło” dostępny na stronie <http://www.odo.umed.wroc.pl/>.
4. Wypełniony i podpisany formularz należy doręczyć inspektorowi ochrony danych w oryginale lub jako skan – plik PDF pod adres iod@umed.wroc.pl
5. Termin powiadomienia: niezwłocznie, najpóźniej w ciągu 24 godzin od stwierdzenia podejrzenia naruszenia ochrony danych osobowych.
6. W przypadku wątpliwości pracownik powinien skonsultować się z inspektorem ochrony danych np. w kwestii poprawnego wypełnienia formularza.

§ 5

Postępowanie inspektora ochrony danych

1. **Ocena, czy podejrzenie naruszenia stanowi naruszenie ochrony danych osobowych.**
	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.
	2. Jeżeli zgłoszone podejrzenie naruszenia nie stanowi naruszenia ochrony danych osobowych w rozumieniu 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 Uczelni).
	3. W przypadku stwierdzenia innego rodzaju naruszeń przepisów o ochronie danych (np. naruszenia zasad, obowiązków informacyjnych itp.) administrator nie ma obowiązku zawiadamiania o tym organu nadzorczego. Inspektor ochrony danych udziela odpowiednich zaleceń w zakresie obowiązków spoczywających na administratorze danych osobowych na mocy obowiązujących przepisów.
2. **Ocena, czy naruszenie ochrony danych skutkuje ryzykiem naruszenia praw lub wolności osoby, której dane dotyczą i udokumentowanie naruszenia.**
	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. W przypadku, gdy:
		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 Uczelni);
		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 Uczelni) zgłoszenie naruszenia Prezesowi Urzędu Ochrony Danych Osobowych w trybie i na zasadach określonych w art. 33 RODO;
		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 Uczelni) zgłoszenie naruszenia 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.
		4. 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.
		5. Wpis do rejestru incydentów, zgodnie z art. 33 ust. 5 RODO zawiera m.in. okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
3. **Zgłoszenie naruszenia ochrony danych organowi nadzorczemu.**
	1. Zgodnie z art. 33 ust. 3 RODO administrator zgłasza zaistniałe naruszenie organowi nadzorczemu 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 pkt 3.1, administrator dokonuje zgłoszenia częściowego, tj. przekazuje informacje, które są znane administratorowi w chwili dokonania zgłoszenia przed upływem 72 godzin, a następnie sukcesywnego uzupełniania zgłoszenia, zgodnie z art. 33 ust. 4 RODO.

**Załącznik Nr 1**

**do Procedury postępowania
z naruszeniem ochrony danych osobowych**

**PRZYKŁADOWY KATALOG NARUSZEŃ I INCYDENTÓW**

**ZAGRAŻAJĄCYCH BEZPIECZEŃSTWU DANYCH OSOBOWYCH**

**1.Formy naruszenia danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych:**

- w zakresie wiedzy:

1) Ujawnienie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym,

2) Ujawnienie informacji o sprzęcie i pozostałej infrastrukturze informatycznej,

3) Dopuszczenie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać, np. z obserwacji lub dokumentacji,

- w zakresie sprzętu i oprogramowania:

1) Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych,

2) Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony,

3) Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci,

4) Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobom nieuprawnionym,

5) Samodzielne instalowanie jakiegokolwiek oprogramowania,

6) Modyfikowanie parametrów systemu i aplikacji,

7) Odczytywanie nośników danych przed sprawdzeniem ich programem antywirusowym,

8) Zaginięcie komputera lub innego nośnika danych (np. telefon, tablet, USB)

- w zakresie dokumentów i obrazów zawierających dane osobowe:

1) Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru,

2) Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych,

3) Nieodpowiednie wyrzucanie dokumentów zawierających dane osobowe,

4) Dopuszczenie do nadmiernego kopiowania dokumentacji i utraty kontroli nad kopią,

5) Dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe,

6) Sporządzanie kopii danych na nośnikach i „wynoszenie” poza obszar ochrony danych bez zgody i wiedzy Administratora,

7) Utrata kontroli nad kopią danych osobowych,

8) Utrata teczki zawierające dane w wersji papierowej,

- w zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych:

1) Dopuszczenie, aby osoby spoza pracowników CI podłączały jakiekolwiek urządzenia do sieci komputerowej, domontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji,

-w zakresie pomieszczeń, w których znajdują się komputery centralne i urządzenia sieci:

1) Dopuszczenie lub ignorowanie faktu, że osoby spoza informatyków dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (korytarze itp.),

2) Dopuszczenie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób nieuprawnionych,

- inne:

1. Zmiana danych bez zgody osoby, której dane dotyczą,
2. Wysłanie danych do niewłaściwej osoby (np. poprzez niewłaściwie zaadresowanie poczty elektronicznej),
3. Nieuprawnione udostępnienie danych (np. elektronicznie – przekazywanie danych przez zdalny dostęp np. VPN, często przydzielane bezterminowo - ale też np. telefonicznie (rozmówca podaje się za pracownika policji czy urzędu, próbując wyciągnąć informacje);
4. Nieodpowiednie usuwanie danych (np. administrator postanawia pozbyć się starych komputerów. Przed sprzedażą usuwa jedynie pliki na pulpicie i opróżnia kosz ze starych plików. Nie usuwa jednak danych z  dysku komputera).

**2. Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych:**

1) Ślady manipulacji przy układach sieci komputerowej lub komputerach,

2) Obecność nowych kabli o nieznanym przeznaczeniu lub pochodzeniu,

3) Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych,

4) Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych,

5) Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe,

6) Wykorzystano niezinwentaryzowany środek przetwarzania informacji (nie będący własnością pracodawcy),

7) Pojawienie się nieautoryzowanej informacji na stronie internetowej.