PROCEDURA	nr: 1/2021	Data: 1.10.2021 r. Wydanie: 1
Procedura zarządzania naruszeniami ochrony danych osobowych w Politechnice Częstochowskiej		

Działając na podstawie art. 33-34, Motywów 85-88 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) oraz w związku z § 27 Polityki ochrony danych osobowych w Politechnice Częstochowskiej, wprowadza się Procedurę zarządzania naruszeniami ochrony danych osobowych w Politechnice Częstochowskiej.

1. **Cel procedury**

   Celem niniejszej procedury jest zapewnienie:

   - wdrożenia zasad wynikających z Polityki ochrony danych osobowych w Politechnice Częstochowskiej,
   - ustalenie szczegółowych zasad zarządzania dokumentacją związaną z naruszeniami danych osobowych,
   - szybkiej i adekwatnej do okoliczności reakcji na wystąpienie lub podejrzenia wystąpienia zdarzenia związanego z naruszeniem ochrony danych osobowych.

2. **Zgłoszenia podejrzenia lub naruszenia ochrony danych osobowych**

   Każdy pracownik jest zobowiązany do zgłoszenia podejrzenia lub naruszenia ochrony danych osobowych zgodnie z załącznikiem nr 5 do obowiązującej Polityki ochrony danych osobowych w Politechnice Częstochowskiej. Zgłoszenie powinno zostać dokonane nie później niż w ciągu 8 godzin od zidentyfikowania zdarzenia do bezpośredniego przełożonego oraz Inspektora Ochrony Danych, a w przypadku gdy zgłoszenie dotyczy przetwarzania danych w systemie teleinformatycznym również do administratora systemu teleinformatycznego.

3. **Działania Inspektora Ochrony Danych w przypadku otrzymania zgłoszenia podejrzenia lub naruszenia ochrony danych osobowych**

   3.1. W przypadku otrzymania zgłoszenia podejrzenia lub naruszenia ochrony danych osobowych Inspektor Ochrony Danych podejmuje następujące działania:

   1) niezwłocznie ustala stan faktyczny dotyczący procesu, w którym doszło lub mogło dojść do zdarzenia, osób odpowiedzialnych za dany proces, rodzaj

zabezpieczeń, które zawiodły, zakresu i liczby danych osobowych, osób których zdarzenie dotyczy oraz możliwych konsekwencji zdarzenia;

2) ustala, jakie działania należy podjąć w celu minimalizacji skutków dla osób fizycznych objętych zdarzeniem;
3) koordynuje proces oceny wagi naruszenia praw i wolności osób fizycznych;
4) zawiadamia rektora o zdarzeniu i wynikach oceny naruszenia praw i wolności osób fizycznych oraz przedstawia rekomendacje dotyczącego dalszego postępowania;
5) przygotowuje, na polecenie rektora, zawiadomienie do Prezesa Urzędu Ochrony Danych Osobowych oraz zawiadomienia osób fizycznych poszkodowanych w wyniku zdarzenia lub jeżeli sytuacja tego wymaga przygotowuje publiczny komunikat w tej sprawie.

3.2. Wszyscy pracownicy są zobowiązani do współpracy z Inspektorem Ochrony Danych w trakcie zbierania materiałów dowodowych oraz wyjaśniania przyczyn zdarzenia i jego skutków dla osób fizycznych.

4. **Ocena wagi naruszenia ochrony danych osobowych**

4.1. Ocenę wagi naruszenia ochrony danych osobowych, zwaną dalej oceną, sporządza się obowiązkowo w przypadku wpłynięcia zgłoszenia dotyczącego podejrzenia lub naruszenia ochrony danych osobowych.

4.2. Ocenę przeprowadza zespół w składzie:

1) Inspektor Ochrony Danych;
2) kierownik jednostki, której dotyczy naruszenie lub podejrzenie naruszenia lub wyznaczony przez niego pracownik;
3) pracownik Biura ochrony danych, informacji niejawnych i bezpieczeństwa,
4) administrator systemu teleinformatycznego - w przypadku, gdy naruszenie jest związane z przetwarzaniem danych w systemie teleinformatycznym.

4.3. Rektor może wskazać inne osoby niż wymienione w pkt. 4.2, które będą uczestniczyć w przeprowadzaniu oceny.

4.4. W ocenie za zgodą Rektora może wziąć udział również przedstawiciel podmiotu przetwarzającego lub współadministratora – w przypadku gdy naruszenie danych osobowych nastąpiło w efekcie działań tych podmiotów.

4.5. Celem oceny jest określenie skutków naruszenia ochrony danych osobowych dla praw i wolności osób fizycznych i przedstawienie rektorowi opinii w kwestii podjęcia działań wynikających z przepisów RODO, dotyczących:

- zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu,

- zawiadomienia osób, których dotyczy naruszenie ochrony danych osobowych,
- wskazania środków w celu przeciwdziałania naruszeniu ochrony danych osobowych oraz zminimalizowania jego negatywnych skutków dla danych podmiotów.

4.6. Ocenę należy przeprowadzić niezwłocznie po otrzymaniu zawiadomienia o podejrzeniu lub naruszeniu ochrony danych osobowych.

4.7. Ocenę przeprowadza się według wytycznych określonych w pkt. 5 i 6 niniejszej procedury.

4.8. Po przeprowadzeniu oceny Inspektor Ochrony Danych sporządza raport, który jest przedstawiany do zatwierdzenia rektorowi w terminie umożliwiającym dokonanie zgłoszenia naruszenia do organu nadzorczego, zgodnie z obowiązującymi przepisami.

4.9. Rejestr naruszeń ochrony danych osobowych oraz dokumentację z tym związaną prowadzi Biuro ochrony danych informacji niejawnych i bezpieczeństwa.

5. **Wytyczne do oceny wagi naruszenia w związku z wystąpieniem podejrzenia lub naruszenia ochrony danych osobowych**

5.1. Niniejsze wytyczne zawierają opis działań oraz wskazówki, jakimi należy się kierować w przypadku podejrzenia lub wystąpienia naruszenia ochrony danych osobowych.

5.2. Ryzyko naruszenia praw lub wolności osób fizycznych powstaje, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Szkodami takimi są np.:

- dyskryminacja,
- kradzież tożsamości lub oszustwo dotyczące tożsamości,
- nadużycia finansowe,
- straty finansowe,
- nieuprawnione cofnięcie pseudonimizacji,
- utrata poufności danych osobowych chronionych tajemnicą zawodową,
- naruszenie dobrego imienia,
- inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej.

Jeżeli naruszenie dotyczy danych osobowych ujawniających:

- pochodzenie etniczne,
- poglądy polityczne,
- przekonania religijne lub światopoglądowe,

- przynależność do związków zawodowych,
- dane genetyczne,
- dane dotyczące zdrowia,
- dane dotyczące życia seksualnego,

należy uznać, że występuje duże prawdopodobieństwo takiej szkody. Niemniej jednak każde z takich zdarzeń należy rozpatrywać indywidualnie.

5.3. Przy dokonywaniu oceny wagi naruszenia stosuje się metodę oceny wagi naruszenia wg Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA).

6. **Metodyka oceny wagi naruszenia**

6.1. Wagę naruszenia (**WN**) określa się za pomocą trzech czynników wg następującego wzoru:

WN = KPD * PI + ON

gdzie:

- **KPD** oznacza kontekst przetwarzania danych. Jest to główny czynnik określający poziom krytyczności zestawu naruszonych danych, w określonym kontekście przetwarzania,
- **PI** oznacza prawdopodobieństwo identyfikacji. Jest to czynnik korygujący KPD, który może obniżyć wynik. Jest to prawdopodobieństwo (łatwość) identyfikacji osoby na podstawie naruszonych danych dla osób, które uzyskały dostęp do nich,
- **ON** oznacza okoliczności naruszenia. Jest to czynnik, który odnosi się do okoliczności naruszenia, które wystąpiły lub nie w danym przypadku.

6.2. Kontekst przetwarzania danych KPD = A + B

Należy oszacować krytyczność związaną z kategorią danych wg czterech poziomów kategorii od 1-4

A – rodzaj i poziom wrażliwości danych

Dane podstawowe = 1

Dane dotyczące zachowań osoby = 2

Dane finansowe = 3

Dane szczególne = 4

B – kontekst przetwarzania, który może podwyższyć lub obniżyć wycenę

Szeroki zakres danych/wolumen danych (+)

Charakter danych (+/-)

Specyfika podmiotu danych lub administratora (+/-)

Możliwe negatywne skutki dla podmiotu danych (+)

Publiczna dostępność danych przed naruszeniem (-)

Nieważność danych (-)

6.3. Prawdopodobieństwo identyfikacji – PI

Należy oszacować jak łatwo będzie podmiotowi, który ma nieuprawniony dostęp do danych zidentyfikować osobę fizyczną, której dane dotyczą. W opisywanej metodologii zostały określone 4 poziomy tej kategorii:

Znikome = 0,25

Ograniczone = 0,5

Wysokie = 0,75

Maksymalne = 1

6.4. Okoliczności naruszenia (ON) ON = NP + NI + ND + IDS

Naruszenie poufności (NP):

Dane ujawnione:

znanej liczbie odbiorców danych (+0,25),

nieznanej liczbie odbiorców danych (+0,5)

Naruszenie integralności (NI):

Dane zmienione i możliwe jest ich odzyskanie (+0,25),

Brak jest możliwości ich odzyskania (+0,5)

Naruszenie dostępności (ND):

Niedostępność danych czasowa (+0,25),

Niedostępność danych pełna i brak możliwości ich odzyskania przez administratora lub podmiot danych (+0,5)

Intencjonalne działanie sprawcy (IDS): (+0,5)

6.5. Ocena wagi naruszenia (WN)

Wynik	Waga naruszenia	Opis
WN<2	Niska	Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności, np. bardzo krótki brak dostępu do danych.
2<=WN	Średnia	Osoby mogą napotkać niedogodności, które są możliwe do pokonania, np. brak dostępu do danych, konieczność ponoszenia dodatkowych kosztów, brak dostępu do usług, stres.

3<=WN<4	Wysoka	Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami, np. umieszczenie osoby na liście dłużników, wezwanie do sądu, długotrwały stres, pogorszenie stanu zdrowia.
4<=WN	Bardzo wysoka	Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje, utrata środków finansowych, niezdolność do pracy, problemy psychiczne itp.

7. Kierownicy jednostek są zobowiązani do zapoznania podległych pracowników z niniejszą procedurą oraz zapewnienia jej przestrzegania w podległych jednostkach.

Inspektor Ochrony Danych
mgr Mariola Ptaszek

Sporządził/-ła: .....

REKTOR
prof. dr hab. inż. Norbert Szygiol
.....
podpis osoby zatwierdzającej

.....
podpis Kwestora*

Marta Kaczmarzyk-Gąsiorek
Radca Prawny
PZ-4862

* Wymagany, jeśli dokument wywołuje skutki finansowe.