PROCEDURA POSTĘPOWANIA Z NARUSZENIAMI

Powiatowego Zespołu Szkół nr 2 im. K. Miarki w Pszczynie

1. Czym jest naruszenie?

Naruszenie ochrony danych osobowych oznacza 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.

Omawiane przypadki występują w szczególności, gdy: stwierdzono kradzież urządzenia (komputery stacjonarne, serwery, urządzenia mobilne, nośniki danych), stwierdzono naruszenie zabezpieczenia systemu informatycznego, stwierdzono występowanie nieautoryzowanych, modyfikacji lub zniszczenia danych, nieautoryzowanego dostęp do danych, udostępnienia ich nieupoważnionym podmiotom lub nielegalnego ujawnienia czy pozyskiwania danych z nielegalnych źródeł.

W organizacji możliwe jest także wystąpienie incydentu bezpieczeństwa danych osobowych, które jest zdarzeniem, które potencjalnie może stanowić lub skutkować naruszeniem ochrony danych osobowych.

2. Ocena wystąpienia naruszenia

Do oceny naruszeń ochrony danych osobowych wyznacza się Inspektora Ochrony Danych Osobowych.

Wśród zadań Inspektora Ochrony Danych Osobowych z zakresu oceny naruszeń należy w szczególności:

a) dokonanie czynności pozwalających na ustaleniu okoliczności powstania zdarzenia;
b) zbieranie materiałów dowodowych dotyczących naruszenia;
c) ustalanie środków i podejmowanie działań mających na celu zabezpieczenie danych osobowych przed kolejnym naruszeniem;
d) ustalanie środków i działań mających zminimalizować negatywne skutki naruszenia;

e) dokumentowanie swoich działań;

f) powiadamianie o naruszeniu Administrator.

3. Postępowanie z naruszeniem

3.1 Obowiązki stwierdzającego wystąpienie incydentu lub podejrzenia wystąpienia naruszenia:

3.1.1 W przypadku stwierdzenia przez upoważnionego do przetwarzania danych osobowych, że mogło mieć miejsce naruszenie przepisów o ochronie danych osobowych ma on obowiązek niezwłocznie zgłosić naruszenie do Inspektora Ochrony Danych Osobowych:

a) numer telefonu do kontaktu: …….

b) adres e-mail do kontaktu: ……..

3.1.2 Następnie stwierdzający potencjalne wystąpienie naruszenia przepisów o ochronie danych osobowych powinien pozostawić miejsce zdarzenia w stanie nienaruszonym do czasu przybycia Inspektora Ochrony Danych Osobowych;

3.1.3 Zawiadomić ochronę zakładu, jeżeli jest to konieczne;

3.1.4 Na żądanie Inspektora Ochrony Danych Osobowych sporządzić pisemne wyjaśnienie dotyczące wykrycia ewentualnego naruszenia, zawierające wszystkie wskazywane okoliczności zdarzenia.

3.2 Obowiązki Inspektora Ochrony Danych Osobowych w trakcie wstępnej oceny zgłoszenia:

3.2.1 Po otrzymaniu zgłoszenia Inspektor Ochrony Danych Osobowych dokonuje wstępnej oceny i analizy okoliczności zdarzenia;

3.2.2 W szczególności Inspektor Ochrony Danych Osobowych sporządza notatki z przeprowadzony oględzin miejsca zgłoszenia;

3.2.3 W razie takiej konieczności sporządza kopię obrazu wyświetlonego na ekranie monitora komputera związanego z naruszeniem, jeżeli jest to konieczne;

3.2.4 Zbiera wywiad i odbiera wyjaśnienia od osoby zgłaszającej naruszenie i osób postronnych;

3.2.5 Dokonuje wszelkich innych, niezbędnych czynności służących właściwemu wyjaśnieniu zdarzenia i oceny potencjalnych skutków naruszenia;

3.2.6 Inspektor Ochrony Danych Osobowych w trakcie podejmowanych przez siebie czynności powinien współpracować i informować na bieżąco o poczynionych ustaleniach Administratora.

3.3 Analiza wystąpienia naruszenia wykonywna przez Inspektora Ochrony Danych Osobowych:

3.3.1 Inspektor Ochrony Danych Osobowych po zebraniu wystarczającego materiału dowodowego dokonuje oceny czy zgłoszone zdarzenie stanowi naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO.

3.3.2 W szczególności Inspektor Ochrony Danych Osobowych w sporządzanym przez siebie raporcie oceniającym wystąpienie zdarzenia analizujemy czy zdarzenie pociąga za sobą możliwość wystąpienia skutków wskazanych w przepisach mogących w szczególności prowadzić do:

a) kradzieży tożsamości;
b) straty finansowej;
c) naruszenia dobrego imienia;
d) naruszenia poufności danych chronionych tajemnicą zawodową;
e) utraty przysługujących osobom praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;
f) ujawnienia danych szczególnych.

3.3.3 Inspektor Ochrony Danych Osobowych powinien dokonać stosownej analizy niezwłocznie, jednakże w czasie nie dłuższym niż 48 godzin od dnia zgłoszenia incydentu czy możliwości wystąpienia naruszenia, chyba że okoliczności sprawy wymagają przedłużenia tego terminu.

3.3.4 Przedłużenie terminu, o którym mowa w pkt 3.3.3 wymaga odnotowania tego faktu w raporcie końcowym wraz ze stosownym uzasadnieniem.

3.4 Czynności podejmowane w trakcie stwierdzenia wystąpienia naruszenia:

3.4.1 W przypadku stwierdzenia naruszenia Inspektor Ochrony Danych Osobowych powiadamia o swoich ustaleniach Administratora przedkładając my stosowny raport;

3.4.2 Administrator lub Inspektor Ochrony Danych Osobowych w imieniu Administratora (zależnie od poczynionych ustaleń) zgłasza bezzwłocznie naruszenie organowi nadzorczemu, jakim jest Urząd Ochrony Danych Osobowych w Warszawie - nie później jednak niż w terminie 72 godzin od stwierdzenia naruszenia, a więc przedłożenia raportu przez Inspektora Ochrony Danych Osobowych;

3.4.3 Naruszenia nie zgłasza się w przypadku stwierdzenia w raporcie przez Inspektora Ochrony Danych Osobowych, że jest mało prawdopodobne, aby naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;

3.4.4 W przypadku przekazania zgłoszenia do organu nadzorczego z opóźnieniem względem terminu wskazanego w pkt 3.4.2 należy załączyć do zgłoszenia przyczyny tego opóźnienia.

3.4.5 Administrator wyciąga konsekwencje dyscyplinarne względem osób, które dokonały naruszenia świadomie lub gdy naruszenie powstało w skutek zawinionego niezachowania reguł ostrożności, do których użytkownik winien był się stosować, a które to zachowanie ograniczyłoby lub wyłączyłoby możliwość wystąpienia naruszenia.

3.4.6 Administrator może wyciągać konsekwencje dyscyplinarne także względem osób, których zachowanie nie wywołało ostatecznie naruszenia, jednakże które w wyniku niestosowania się do obowiązujących reguł i zasad postępowania w zakresie ochrony danych osobowych w placówce narażają swoją pracą dane osobowe i mogą lub doprowadzają do uchybień i incydentów.

4. Zgłoszenie naruszenia

4.1 Zgłoszenie do organu nadzorczego musi zawierać co najmniej:

a) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) imię i nazwisko oraz dane kontaktowe Inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
d) opis środków zastosowanych lub proponowanych przez Administrator w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

5. Powiadomienie osoby, której dane dotyczą

5.1 W przypadku stwierdzenia naruszenia przepisów o ochronie danych osobowych, które mogą skutkować wysokim ryzykiem naruszenia praw i wolności osoby, której dane zostały objęte naruszeniem, Administrator lub Inspektor Ochrony Danych Osobowych w imieniu Administratora (zależnie od poczynionych ustaleń) zawiadamia o takim naruszeniu osobę, której dane dotyczą.

5.2 Administrator odstępuje od zawiadomienia osób o zaistniałym naruszeniu ochrony danych, jeżeli dokonana przez Inspektor Ochrony Danych Osobowych ocena wykazuje, że:

a) naruszenie przepisów o ochronie danych nie stanowi naruszenia ochrony danych osobowych lub gdy jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;
b) naruszenie danych osobowych dotyczyło danych, przy których wdrożono odpowiednie środki techniczne i organizacyjne, w szczególności takie jak szyfrowanie uniemożliwiające odczyt danych osobowych przez osoby nieuprawnione.

5.3 Zawiadomienie, o którym mowa w pkt 5.1 musi zostać przekazane jasnym i prostym językiem, jednocześnie opisując charakter naruszenia ochrony danych osobowych.

5.4 Zawiadomienie, o którym mowa w pkt 5.1 powinno zawierać co najmniej:

a) imię i nazwisko oraz dane kontaktowe Inspektor Ochrony Danych Osobowych 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.

5.5 Jeżeli naruszenie danych osobowych dotyczy wielu osób Administrator wyda publiczny komunikat lub zamieści stosowny komunikat na stronie internetowej Szkoły.

6. Szczegółowe wytyczne i wskazówki postępowania dla Inspektora Ochrony Danych Osobowych

6.1 Oznaczanie zdarzeń:

a) Uchybienie – jest to świadome lub nieświadome działanie, wskutek których **może dojść** do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych;

b) Naruszenie – jest to świadome lub nieświadome działanie, wskutek których **doszło** do utraty danych osobowych, kradzieży danych osobowych lub uszkodzenia nośników danych.

6.2 Inspektor Ochrony Danych Osobowych w ramach podejmowanej analizy zgłoszenia ma za zadanie rozpoznać wystąpienia uchybienia lub naruszenia i w każdym przypadku ma obowiązek:

6.2.1 W przypadku stwierdzenia **uchybienia**:

6.2.1.1 Odnotować każde uchybienie w odpowiednim arkuszu Rejestru naruszeń.

6.2.1.2 W trakcie wypełniania Rejestru naruszeń Inspektor Ochrony Danych Osobowych powinien posiłkować się załączoną poniżej „Tabelą uchybień i zagrożeń”.

6.2.1.3 Sporządzić „Protokół Uchybienia” wg załączonego poniżej wzoru.

6.2.1.4 Wprowadzić procedury lub podjąć działania uniemożliwiające ponowne powstanie uchybienia.

6.2.2 W przypadku stwierdzenia **naruszenia**:

6.2.2.1 Zabezpieczyć dane osobowe, nośniki danych i wszelkie inne możliwe do zabezpieczenia dowody.

6.2.2.2 Odnotować każde naruszenie w odpowiednim arkuszu Rejestru naruszeń.

6.2.2.3 W trakcie wypełniania Rejestru naruszeń Inspektor Ochrony Danych Osobowych powinien posiłkować się załączoną poniżej „Tabelą uchybień i zagrożeń”.

6.2.2.4 Sporządzić „Raport z naruszenia” wg załączonego poniżej wzoru.

6.2.2.5 Po zakończeniu wszelkich pozostałych, wymaganych prawem procedur, w tym w szczególności po powiadomieniu Administratora oraz przy współpracy z Administratorem po powiadomieniu organu nadzorczego, a w niektórych przypadkach także osoby, której dane dotyczyły, Inspektor Ochrony Danych Osobowych powinien przygotować propozycje procedur, działań i/lub rozwiązań, które należałoby wprowadzić celem uniemożliwienia ponownego wystąpienia naruszenia.

6.2.2.6 Po zakończeniu pozostałych procedur, niezbędnych do podjęcia w przypadku stwierdzenia naruszenia, w tym w szczególności po konsultacji z organem nadzorczym, Inspektor Ochrony Danych Osobowych współdziałając z Administratorem powinien podjąć próbę przywrócenia stanu sprzed zaistnienia zagrożenia.

TABELA UCHYBIEŃ I ZAGROŻEŃ

Kod uchybienia lub zagrożenia	Uchybienia i zagrożenia nieświadome wewnętrzne i zewnętrzne
01	Pomieszczenie, w którym przechowywane są dane osobowe pozostaje bez nadzoru.
02	Komputer nie jest zabezpieczony hasłem.
03	Dostęp do danych osobowych mają osoby nieposiadające upoważnienia.
04	Nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym.
05	Próba kradzieży lub kradzież danych osobowych przetwarzanych w formie elektronicznej.
06	Próba kradzieży lub kradzież danych osobowych w formie papierowej (łącznie z kradzieżą pośrednią, np. kradzież samochodu z dokumentami w środku)
07	Nieuprawniony dostęp do danych osobowych w formie papierowej.
08	Dane osobowe przechowywane są w niezabezpieczonym pomieszczeniu.
09	Próba włamania do pomieszczenia/budynku.
10	Działanie zewnętrznych aplikacji, wirusów, złośliwego oprogramowania.
11	Brak aktywnego oprogramowania antywirusowego.
12	Zniszczenie lub modyfikacja danych osobowych w formie papierowej.

13	Zniszczenie lub modyfikacja danych osobowych w systemie informatycznym.
14	Uszkodzenie komputerów, nośników danych.
15	Próba nieuprawnionej interwencji przy sprzęcie komputerowym.
16	Zdarzenia losowe.
17	Podejrzane (nietypowe) działanie komputera lub sprzętu.
18	Próba wyłudzenia lub wyłudzenie informacji przez osobę nieuprawnioną (telefonicznie, mailowo, osobiście)
19	Zagubienie nośnika danych osobowych (dokumentu, dysku, komórki, komputera)
20	Nieuprawnione udostępnienie danych (np. przesłanie wiadomości e-mail na niepoprawny adres, niepoprawne zaadresowanie poczty tradycyjnej)

Pszczyna, dnia …….. r.

Inspektor Ochrony Danych Osobowych:

…….

…….

…….

PROTOKÓŁ UCHYBIENIA

Powiatowy Zespół Szkół nr 2 im. K. Miarki w Pszczynie

Data i godzina wystąpienia uchybienia: .....

Miejsce wystąpienia uchybienia:.....

Kod uchybienia (i/lub informacja dot. charakteru uchybienia): .....

.....

Szczegółowy opis uchybienia:

.....

.....

.....

.....

Przyczyny powstania uchybienia:

.....

.....

.....

.....

Skutki uchybienia:

.....

.....

.....

.....

Podjęte działania naprawczo-zapobiegawcze:

.....

.....

.....

.....

Uwagi dodatkowe:

.....

.....

.....

.....

…….. ……..
Inspektor Ochrony Danych Osobowych Administrator

Pszczyna, dnia …….. r.

Inspektor Ochrony Danych Osobowych:

…….

…….

…….

RAPORT Z NARUSZENIA

Powiatowy Zespół Szkół nr 2 im. K. Miarki w Pszczynie

Data i godzina wystąpienia naruszenia: .....

Miejsce wystąpienia naruszenia:.....

Kod naruszenia (i/lub informacja dot. charakteru naruszenia): .....

.....

Szczegółowy opis naruszenia:

.....

.....

.....

.....

Przyczyny powstania naruszenia:

.....

.....

.....

.....

Skutki naruszenia:

.....

.....

.....

.....

Podjęte działania naprawczo-zapobiegawcze:

.....

.....

.....

.....

Uwagi dodatkowe:

.....

.....

.....

.....

…….. ……..
Inspektor Ochrony Danych Osobowych Administrator