PROCEDURA
DOTYCZĄCA INCYDENTÓW I NARUSZEŃ OCHRONY DANYCH OSOBOWYCH W SZKOLE PODSTAWOWEJ Z ODDZIAŁAMI INTEGRACYJNYMI NR 11 IM. BOLESŁAWA CHROBREGO W PŁOCKU

Administrator Danych Osobowych: Szkoła Podstawowa z Oddziałami Integracyjnymi nr 11 im. Bolesława Chrobrego w Płocku, ul. Kochanowskiego 11, 09-402 Płock

Inspektor Ochrony Danych: Tomasz Skwarski, iod@zjoplock.pl, tel. 24 367 89 34.

1. 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.
2. Identyfikując incydent w sferze bezpieczeństwa danych osobowych, Administrator zobowiązany jest przeanalizować całość procesów z nim związanych.
3. Obowiązki administratora dotyczące naruszeń ochrony danych osobowych.
    1) Administrator prowadzi nadzór nad przestrzeganiem wewnętrznych procedur, które umożliwią jak najwcześniejsze wyłapywanie naruszeń lub działań ryzykownych mogących do tych naruszeń doprowadzić:
        a) zobowiązuje pracowników do niezwłocznego zgłaszania wszelkich zidentyfikowanych naruszeń i sytuacji mogących do nich doprowadzić,
        b) określa system obiegu informacji: w pierwszej kolejności pracownicy zgłaszają informacje do dyrektora szkoły, który podejmuje dalsze decyzje,
        c) przestrzega zasady weryfikacji procesów przetwarzania danych w organizacji, zwłaszcza jeśli następują w nich jakieś zmiany,
        d) weryfikuje umowy powierzenia zawarte z firmami świadczącymi usługi outsourcingowe, tak aby znalazły się w nich zapisy zgodne z art. 28 RODO dotyczące niezwłocznego informowania administratora o naruszeniach zidentyfikowanych przez procesora.
    2) Administrator organizuje szkolenia mające ułatwić pracownikom rozpoznawanie naruszeń i identyfikację sytuacji mogących do tych naruszeń prowadzić, a także zwiększyć świadomość pracowników co do wagi tego zagadnienia.
    3) Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze prowadząc wewnętrzną ewidencję. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania artykułu 33 ust. 5 RODO.
    4) Przed podjęciem decyzji o tym, czy dane naruszenie zgłaszać do organu nadzorczego, administrator jest zobowiązany dokonać analizy skutków zidentyfikowanego naruszenia dla podmiotów danych:
        a) ocenić, jakie ryzyko dla osób, których dane dotyczą, niesie za sobą ich nieprawne ujawnienie osobom nieupoważnionym,
        b) w jaki sposób naruszenie ich integralności może wpłynąć na osoby, których te dane dotyczą,
        c) jakie jest prawdopodobieństwo, że na skutek wystąpienia tych naruszeń osoby te mogą być narażone na dyskryminację, naruszenie ich dobrego imienia, kradzież ich tożsamości, negatywne skutki finansowe, ograniczenie ich praw i wolności.
    5) Przyjmuje się, że jeśli naruszenie dotyczy danych wrażliwych, wówczas ryzyko wystąpienia negatywnych skutków dla osób, których te dane dotyczą, z założenia jest duże.
    6) Zgłoszenie naruszenia kierowane jest do Prezesa Urzędu Ochrony Danych Osobowych (Prezes UODO).

7) Do Urzędu Ochrony Danych Osobowych należy zgłaszać tylko te naruszenia, które w ocenie administratora niosą ze sobą duże ryzyko wystąpienia negatywnych skutków dla praw i wolności osób, których dane dotyczą.
8) Zgłoszeń naruszenia należy dokonywać bez zbędnej zwłoki, w ciągu maksymalnie 72 godzin od momentu pozyskania wiedzy o wystąpieniu naruszenia w formie elektronicznej, za pomocą formularza znajdującego się na stronie https://uodo.gov.pl.
9) W sytuacji, gdy administrator nie będzie w stanie w wyznaczonym terminie (72 godziny) przekazać do Urzędu kompletu informacji o naruszeniu, może przesyłać je cyklicznie – jest to jednak uwarunkowane dostarczeniem wyjaśnienia, dlaczego nie jest w stanie wywiązać się z nałożonego na niego zobowiązania.
10) Administrator wskazuje w zgłoszeniu naruszenia co najmniej następujące informacje:
    a) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą,
    b) kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
    c) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych, od którego można uzyskać więcej informacji,
    d) opis możliwych konsekwencji naruszenia ochrony danych osobowych,
    e) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków zastosowanych w celu zminimalizowania jego ewentualnych negatywnych skutków.
11) Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia o takim naruszeniu osobę, której dane dotyczą.
12) Zawiadomienie opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO.
13) Zawiadomienie 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) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
    c) przygotowanie zawiadomienia wymagałoby 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.
14) Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 13.

5. Wdrożenie zmian w celu zapobieżenia ponownemu wystąpieniu naruszenia.
    1. Po wykryciu naruszenia administrator jest zobowiązany przeanalizować przyczyny jego wystąpienia, następnie zmodyfikować procedury w zakresie przetwarzania danych osobowych, a także zastosować środki organizacyjne i techniczne tak dobrane, aby wykluczyć powtórzenie się scenariusza, w którym doszło do naruszenia ochrony danych osobowych.
    2. Wskazane jest przeprowadzenie dodatkowego szkolenia pracowników lub wprowadzenie dodatkowych zabezpieczeń w postaci szyfrowania dokumentów, pseudonimizacja danych,

zmodyfikowanie procesu obiegu dokumentów – aby wyeliminować lub ograniczyć wystąpienie zidentyfikowanych zagrożeń.

6. Szczegółowe regulacje dotyczące działań w przypadku stwierdzenia naruszenia ochrony danych osobowych zawiera *Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych*.

Załączniki:

Nr 1: przykłady sytuacji wymagających zgłoszenia naruszenia przez pracowników.

Nr 2: wzór zgłoszenia naruszenia UODO.

Nr 3: instrukcja postępowania w przypadku naruszenia ochrony danych osobowych.

Załącznik nr 1
do Procedury dotyczącej incydentów i naruszeń
ochrony danych osobowych

Przykłady sytuacji wymagających zgłoszenia naruszenia przez pracowników

1. Próby wyłudzenia informacji na temat identyfikatorów i haseł do logowania (*phishing* – próba pozyskania informacji drogą email, przez telefon, w bezpośredniej rozmowie).
2. Hasła dostępu trzymane w widocznych, dostępnych dla innych miejscach.
3. Przebywanie osób nieupoważnionych w miejscach przetwarzania danych osobowych.
4. Wyrzucanie dokumentów, notatek z danymi osób fizycznych bez korzystania z niszczarek.
5. Umożliwienie dostępu osobom nieupoważnionym do danych osobowych poprzez pozostawienie wydruków na drukarkach, pozostawienie osób nieupoważnionych w pomieszczeniu, gdzie np. na biurkach były pozostawione dokumenty zawierające dane osobowe.
6. Kradzież/zagubienie niezabezpieczonego hasłem komputera, nośnika danych (dysku zewnętrznego, pendrive'a), teczek z dokumentami.
7. Zidentyfikowanie złośliwego oprogramowania na komputerze.
8. Przesłanie wiadomości e-mail zawierającej dane osobowe do wielu adresatów bez opcji UDW lub do niewłaściwego adresata w wersji niezaszyfrowanej.

Uwagi

Ważne, aby pracownicy zgłaszali takie zdarzenia administratorowi, aby ten mógł wypełnić nałożone przez przepisy obowiązki dotyczące oceny ryzyka dla osób, których dane zostały ujawnione, i w zależności od jej wyników podjąć decyzję o konieczności zgłoszenia naruszenia do organu nadzorczego i konieczności powiadomienia o nim osób, których dane zostały ujawnione osobom nieupoważnionym.

Załącznik nr 2
do Procedury dotyczącej incydentów i naruszeń
ochrony danych osobowych

Płock, dn. …….

(miejscowość, data)

Administrator danych osobowych

……

Urząd Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

Zgłoszenie
w sprawie naruszenia ochrony danych osobowych

Niniejszym w trybie art. 33 ogólnego rozporządzenia o ochronie danych zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu …… w Szkole Podstawowej z Oddziałami Integracyjnymi nr 11 im. Bolesława Chrobrego w Płocku, ul. Kochanowskiego 11.

Charakter naruszenia ochrony danych	Np. *Przesłanie przez pracownika wiadomości e-mail do błędnego adresata (nieznana osoba) zamiast do współpracownika, wraz z załącznikiem w formacie pliku Excel (niezabezpieczonego) zawierającym dane rodziców i wychowanków (takie jak: imię i nazwisko, adres zamieszkania, PESEL, nr dowodu tożsamości, numer telefonu, adresy e-mail)*
Kategoria i przybliżona liczba osób, których dane dotyczą	Np. *Wychowankowie, rodzice. Liczba osób, których dane dotyczą .....*
Liczba wpisów, których dotyczy naruszenie	Np. *821*
Możliwe konsekwencje naruszenia ochrony danych	Np. *Powstanie szkód majątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub kradzież lub sfałszowanie tożsamości, strata finansowa*
Środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych	Np. *Wdrożenie stosownych środków kryptograficznych, w tym pseudonimizacja, zakaz przesyłania załączników zawierających dane osobowe w sposób niezabezpieczony*
Dane inspektora ochrony danych	Np. *....., nr telefonu: XXX XXX XXX, adres e-mail: iod@domena.pl*

……
……..……*

……

(podpis dyrektora)

*W przypadku zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin, administrator danych zobowiązany jest do złożenia wyjaśnień w przedmiocie przyczyn opóźnienia.