ZJO
ZARZĄD JEDNOSTEK OŚWIATOWYCH
JEDNOSTKA BUDŻETOWA

Zarządzenie Nr 10/2018

Dyrektora Zarządu jednostek Oświatowych - JB w Płocku

z dnia 07.12.2018 r.

w sprawie: wprowadzenia Instrukcji postępowania w sytuacjach naruszenia ochrony danych osobowych w Zarządzie Jednostek Oświatowych - JB w Płocku.

Na podstawie art. 24 ust. 1 i 2 w zw. z art. 33 i 34 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 (Dz. U. UE L z 2016 r. Nr 119, str. 1) zarządzam, co następuje:

§ 1

Wprowadzam „Instrukcję postępowania w sytuacjach naruszenia ochrony danych osobowych w Zarządzie Jednostek Oświatowych - JB w Płocku" stanowiącą Załącznik do niniejszego Zarządzenia.

§2

Zobowiązuje się wszystkich pracowników Zarządu Jednostek Oświatowych - Jednostka Budżetowa w Płocku, do zapoznania się z niniejszym Zarządzeniem i Załącznikiem nr 1 do zarządzenia oraz przestrzegania zasad w nich zawartych.

§ 3

Nadzór nad wykonaniem zarządzenia powierzam Inspektorowi Ochrony Danych w ZJO w Płocku.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Zarządu Jednostek Oświatowych - JB
Maciej Krzemiński

Inspektor Ochrony Danych
Zarząd Jednostek Oświatowych
- JB w Płocku
Tadeusz Borowicki

RADCA PRAWNY
Sylwia Wachnowicz

ZJO
ZARZĄD JEDNOSTEK OŚWIATOWYCH
JEDNOSTKA BUDŻETOWA

Załącznik do Zarządzenia Nr 10/2018
Dyrektora Zarządu Jednostek Oświatowych–
Jednostka Budżetowa w Płocku
z dnia 07 grudnia 2018 roku

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Wstęp

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz.U. UE L z 2016 r. Nr 119, s. 1) [dalej **RODO**] nakłada na Administratora Danych Osobowych (Zarząd Jednostek Oświatowych – Jednostka Budżetowa w Płocku, reprezentowany przez Dyrektora) określone wymagania dotyczące postepowania w sytuacji naruszenia ochrony danych osobowych. Obowiązki te obejmują:

1. zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 ust. 1–4 RODO);
2. dokumentowanie naruszeń ochrony danych osobowych (art. 33 ust. 5 RODO);
3. zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34 RODO).

§ 1

Cel i przedmiot Instrukcji

1. Celem wprowadzenia niniejszej Instrukcji jest ustalenie:
   a. katalogu zdarzeń, które mogą stanowić lub prowadzić do naruszenia ochrony danych osobowych;
   b. wytycznych dotyczących prawidłowego reagowania pracowników ZJO w sytuacjach stanowiących naruszenie ochrony danych lub do niego prowadzących oraz nieprawidłowości w zakresie zabezpieczeń systemu informatycznego;
   c. procedury prowadzenia wewnętrznej dokumentacji rejestrującej wszelkie naruszenia ochrony danych osobowych;
   d. procedury zgłaszania naruszeń ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych (dalej PUODO);
   e. procedury na wypadek wystąpienia zdarzeń powodujących wysokie ryzyko naruszenia praw i wolności osób, w zakresie informowania ich o takim zdarzeniu oraz podjęcia czynności zaradczych;

f. zadań i roli Inspektora Ochrony Danych w zakresie realizacji ww. celów.

2. Powyższe ustalenia dokonywane są z uwzględnieniem specyfiki funkcjonowania ZJO.

§2

Istota naruszenia ochrony danych osobowych

1. Przez pojęcie **„naruszenie ochrony danych"** rozumie się 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. Na potrzeby niniejszego dokumentu wyróżniono dwa typy zdarzeń:
   a. stanowiące naruszenie - definiowane jako naruszenie bezpieczeństwa danych osobowych ze względu na poufność, integralność i dostępność do przetwarzania danych, zwane dalej incydentem;
   b. mogące prowadzić do naruszenia - zagrożenie bezpieczeństwa danych osobowych, które należy rozumieć jako potencjalną możliwość (podatności) wystąpienia incydentu, zwane dalej zagrożeniem.
3. Nieprawidłowości w zakresie systemu ochrony danych osobowych mogą zostać stwierdzone, w szczególności, na podstawie oceny:
   a. stanu urządzeń technicznych;
   b. zawartości zbiorów danych osobowych;
   c. sposobu działania urządzeń i programu lub jakości komunikacji w sieci teleinformatycznej;
   d. sposobu pracy (w tym obiegu dokumentów);
   e. stanu pomieszczeń wchodzących w skład obszaru przetwarzania danych oraz ich wyposażenia;
   f. wyglądu stanowiska pracy.

§3

Postępowanie w przypadku naruszeń ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych lub zobowiązana do zachowania poufności danych osobowych w przypadku stwierdzenia zaistnienia podatności (zagrożenia) lub wystąpienia incydentu, zobowiązana jest bezzwłocznie poinformować o tym fakcie Inspektora Ochrony Danych.
2. Katalog zagrożeń i incydentów oraz zalecanych reakcji stanowi Załącznik nr 1.
3. Obowiązki pracownika w związku ze stwierdzeniem zagrożenia naruszenia ochrony danych osobowych:
   a. pozostanie na miejscu zdarzenia do momentu przybycia Inspektora Ochrony Danych, stanowisko można opuścić tylko w uzasadnionych przypadkach;
   b. podjęcie czynności niezbędnych do powstrzymania skutków naruszenia;
   c. zabezpieczenie dowodów umożliwiających ustalenie przyczyn, sprawcy i skutków

zdarzania, w formie zapamiętania lub zanotowania wszystkich ważnych szczegółów dotyczących zajścia (np. typ niezgodności lub naruszenia, błąd działania, wiadomość z ekranu, dziwne zachowanie itp.);

d. zaniechanie wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia.

4. Administrator Systemów Informatycznych jest zobowiązany do informowania Inspektora Ochrony Danych o wszelkich anomaliach w pracy administrowanych przez siebie systemów i urządzeń, mogących być przyczyną lub skutkiem incydentu lub zagrożenia w zakresie danych osobowych.

§ 4

Działania Inspektora Ochrony Danych

1. Inspektor Ochrony Danych po otrzymaniu informacji o możliwym naruszeniu, rozpoznaje sytuację oraz zapoznaje się z relacją osoby powiadamiającej, jak i również innych osób, które mogą posiadać informacje o zaistniałym zdarzeniu. Następnie podejmuje decyzję odnoszącą się do dalszego postępowania.
2. Inspektor Ochrony Danych przeprowadza ocenę możliwego ryzyka dla osób fizycznych, pozwalającą stwierdzić, czy powstał wymóg powiadomienia organu nadzorczego oraz osób, których dane dotyczą, a także określa konieczne działania do zaradzenia naruszeniu.
3. Jeśli w wyniku przeprowadzonych czynności wyjaśniających Inspektor Ochrony Danych uzna, że doszło do naruszenia ochrony danych osobowych należy powiadomić o tym zdarzeniu organ nadzorczy.
4. W przypadku stwierdzenia naruszenia ochrony danych osobowych przez Inspektora Ochrony danych prowadzi on postępowanie wyjaśniające w toku, którego:
   a. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
   b. zabezpiecza ewentualne dowody,
   c. ustala osoby odpowiedzialne za naruszenie,
   d. inicjuje działania porządkowe wobec osób odpowiedzialnych za naruszenia,
   e. podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
   f. wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
   g. dokumentuje prowadzone postępowania sporządzając raport (wzór zawiera Załącznik nr 2a).
5. W przypadku stwierdzenia wystąpienia zagrożenia, Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające w toku, którego:
   a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
   b. sugeruje podjęcie ewentualnych działań porządkowych wobec pracowników,

c. podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),

d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,

e. dokumentuje prowadzone postępowanie sporządzając raport (wzór zawiera Załącznik nr 2b).

6. Inspektor Ochrony Danych ewidencjonuje przypadki wystąpienia zagrożeń i incydentów (naruszeń) ochrony danych osobowych, uwzględniając opis podjętych działań zapobiegawczych i naprawczych w celu minimalizacji skutków wystąpienia zdarzania (wzór ewidencji zawiera Załącznik nr 3).

7. Dokumentację ewidencjonującą zaistniałe zagrożenia i incydenty przechowuje Inspektor Ochrony Danych w metalowej szafie zamykanej na klucz w zamykanym pomieszczeniu.

§ 5

Zgłaszanie naruszeń do organu nadzorczego

1. W razie stwierdzenia przez Inspektora Ochrony Danych naruszenia ochrony danych osobowych, Administrator danych osobowych zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych bez zbędnej zwłoki – jednak nie później niż w terminie 72 godzin od stwierdzenia naruszenia.

2. Zgłoszenie naruszenia ochrony danych osobowych (na podstawie raportu Inspektora Ochrony Danych) powinno zawierać:
   a. opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie 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;
   c. opis możliwych skutków naruszenia ochrony danych osobowych;
   d. opis środków technicznych i organizacyjnych zastosowanych przez Administratora danych osobowych w celu zaradzenia naruszeniu ochrony danych osobowych oraz minimalizacji jego ewentualnych negatywnych skutków.
3. PUODO nie powiadamia się:
   a. gdy jest mało prawdopodobne, by incydent skutkował ryzykiem naruszenia praw lub wolności osób fizycznych;
   b. jeżeli miało miejsce jedynie zagrożenie, a nie naruszenie;
4. Sytuacje, w których dochodzi do naruszenia obejmują przypadki wystąpienia:
   a. utraty kontroli nad przetwarzanymi danymi;
   b. zagrożenia praw i interesów osób, których dane dotyczą;
   c. negatywnych konsekwencji wizerunkowych;
   d. negatywnego odbioru społecznego związanego z upublicznieniem danych osobowych.
5. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu odbywa się drogą elektroniczną, przy pomocy udostępnionego przez Urząd Ochrony Danych Osobowych formularza elektronicznego.

§ 6

Zawiadamianie osób, których dane dotyczą

1. W przypadku gdy incydent wymaga powiadomienia PUODO, Administrator danych osobowych bez zbędnej zwłoki zawiadamia również osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie w prosty sposób opisuje charakter naruszenia ochrony danych osobowych oraz zawiera następujące elementy:
   a. imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych;
   b. opis możliwych negatywnych skutków naruszenia ochrony danych osobowych,
   c. opisywać środki techniczne i organizacyjne zastosowane przez Administratora danych osobowych w celu zaradzenia naruszeniu ochrony danych osobowych oraz minimalizacji jego ewentualnych negatywnych skutków
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
   a. Administrator danych osobowych wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie,
   b. Administrator danych osobowych zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
   c. 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.

§7

Odpowiedzialność

1. Wobec pracownika, który w przypadku wystąpienia incydentu lub zagrożenia bezpieczeństwa danych osobowych nie podjął działań przewidzianych w niniejszej instrukcji, a w szczególności nie powiadomił właściwej osoby, możliwe jest podjęcie czynności porządkowych.
2. Kara porządkowa nałożona na pracownika nie wyklucza poniesienia przez niego odpowiedzialności zgodnie z obowiązującymi przepisami.

Inspektor Ochrony Danych
Zarząd Jednostek Oświatowych
- JB w Płocku
Tadeusz Borowicki

DYREKTOR
Zarządu Jednostek Oświatowych - JB
Maciej Krzemiński

Załącznik do Zarządzenia Nr 10/2018
Dyrektora Zarządu Jednostek Oświatowych– Jednostka Budżetowa w Płocku
z dnia 07 grudnia 2018 roku

Załącznik nr 1

Tabela form naruszeń bezpieczeństwa danych osobowych

Zagrożenie lub incydent w zakresie danych osobowych		
A	**W OBSZARZE PROCEDUR, SPRZĘTU ORAZ SYSTEMÓW**	
	Rodzaj zdarzenia	**Zalecane postępowania pracownika**
1.	Ujawnienie:	
a)	sposobu działania systemu oraz zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić Inspektora Ochrony Danych
b)	informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić Inspektora Ochrony Danych.
c)	danych osobowych przez wiadomość e-mail wysłaną do niewłaściwego adresata	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa. Powiadomić Inspektora Ochrony Danych
d)	otwartej adresatów nie będących pracownikami ZJO przez wysłanie zbiorowych wiadomości email	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa. Powiadomić Inspektora Ochrony Danych.
e)	informacji o uczniu/dziecku lub pracowniku nieupoważnionym lub niezweryfikowanym odbiorcom	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Powiadomić Inspektora Ochrony Danych
2.	Dopuszczenie do:	
a)	korzystania z aplikacji i urządzeń umożliwiające dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba upoważniona.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Przekazać informację do Inspektora Ochrony Danych
b)	użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nieupoważnione.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska pracy. Ustalić jakie czynności zostały wykonane. Powiadomić Inspektora Ochrony Danych.
c)	zmiany konfiguracji sprzętowej oraz programowej systemów oraz stacji roboczych przez niepowołane osoby.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić Inspektora Ochrony Danych i Administratora Systemu Informatycznego
3.	Wykorzystywanie:	
a)	ogólnodostępnych serwisów pocztowych w celach służbowych (np. Wirtualna Polska, Onet.pl, o2.pl) bez zgody Administratora Systemu Informatycznego.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić Inspektora Ochrony Danych.
b)	służbowej poczty elektronicznej do celów prywatnych.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Powiadomić Inspektora Ochrony Danych.

4.	Pozostawienie:	
a)	otwartego systemu po opuszczeniu stanowiska pracy umożliwiając dostęp do bazy danych osobowych	Niezwłocznie zakończyć działanie systemu lub zablokować komputer. Przekazać informację do Inspektora Ochrony Danych.
b)	zapisanego hasła w jakimkolwiek widocznym miejscu.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić Inspektora Ochrony Danych.
5.	Odczytywanie nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy.
6.	Samodzielne instalowanie i wykorzystanie nielegalnego oprogramowania	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić Inspektora Ochrony Danych.
7.	Stwarzanie warunków, aby ktokolwiek mógł pozyskać informację o sprzęcie i pozostałej infrastrukturze informatycznej np. z obserwacji lub dokumentacji.	Natychmiast przerwać czynność prowadzącą do ujawnienia informacji. Powiadomić Inspektora Ochrony Danych.
8.	Niezapowiedziane zmiany w wyglądzie lub zachowaniu systemu zawierającego dane osobowe	Powiadomić niezwłocznie Administratora Systemu Informatycznego i Inspektora Ochrony Danych. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.
9.	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	Powiadomić niezwłocznie Administratora Systemu Informatycznego. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.
10	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	Powiadomić niezwłocznie Administratora Systemu Informatycznego i Inspektora Ochrony Danych. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.
11	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe	Powiadomić niezwłocznie Inspektora Ochrony Danych.
12	Przechowywanie haseł w niewłaściwy sposób.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić Inspektora Ochrony Danych.
13	Przekazywanie haseł innym osobom.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Niezwłocznie powiadomić Inspektora Ochrony Danych.
14	Wykorzystanie służbowych środków przetwarzania informacji do celów prywatnych.	Powiadomić niezwłocznie Inspektora Danych Osobowych. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji
15	Fizyczne zniszczenie lub uszkodzenie sprzętu oraz nośników przetwarzających informacje.	Powiadomić niezwłocznie Administratora Systemu Informatycznego i Inspektora Ochrony Danych. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.
16	Kradzież sprzętu przetwarzającego informacje.	Niezwłocznie powiadomić Administratora Systemu Informatycznego i Inspektora Ochrony Danych.
17	Błędy w obsłudze sprzętu komputerowego służącego do przetwarzania informacji.	Powiadomić niezwłocznie Administratora Systemu Informatycznego i Inspektora Ochrony Danych. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.
18	W wyniku rozwiązania umowy z pracownikiem nie podjęto działań związanych z odebraniem uprawnień.	Powiadomić niezwłocznie Administratora Systemu Informatycznego. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji.

B	W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	
	Rodzaj zdarzenia	**Zalecane postępowania pracownika**
1.	Pozostawienie:	
a)	dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Przekazać informację do Inspektora Ochrony Danych.
b)	dokumentacji zawierającej dane osobowe pracowników, uczniów, dzieci, rodziców w ogólnodostępnym miejscu	Zabezpieczyć dokumenty. Przekazać informacje do Inspektora Ochrony Danych.
2.	Dopuszczenie:	
a)	do kopiowania dokumentów i utraty ich kopii.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć kopię. Powiadomić Inspektora Ochrony Danych.
b)	aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor.
3.	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić Inspektora Ochrony Danych.
4.	Sporządzanie kopii danych na zewnętrznych nośnikach danych bez zgody Administratora Systemu Informatycznego.	Spowodować zaprzestanie kopiowania. Odzyskać i wykonaną kopię. Powiadomić Inspektora Ochrony Danych i Administratora Systemu Informatycznego
5.	Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić Inspektora Ochrony Danych.
6.	Wynoszenie dokumentów i nośników danych z ZJO bez zabezpieczeń oraz zobowiązań pracowników.	Wezwać osobę do bezwzględnego zaniechania tego. Powiadomić Inspektora Ochrony Danych.
C	W OBSZARZE INFRASTRUKTURY	
	Rodzaj zdarzenia	**Zalecane postępowania pracownika**
1.	Pozostawienie:	
a)	Pozostawienie otwartych okien, drzwi po zakończeniu pracy.	Zabezpieczyć (zamknąć) pomieszczenie.
b)	Pozostawienie dokumentów w koszu na śmieci.	Zabezpieczyć dokumenty. Przekazać informację do Inspektora Ochrony Danych
c)	Pozostawienie wydruków na ogólnodostępnej drukarce.	Zabezpieczyć dokumenty. Przekazać informację do Inspektora Ochrony Danych
2.	Opuszczenie i pozostawienie bez dozoru niezamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy do przetwarzania danych osobowych.	Zabezpieczyć (zamknąć) pomieszczenie.
3.	Ignorowanie lub dopuszczenie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiekolwiek urządzenia do sieci komputerowej, demontowały elementy obudów do gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Powiadomić Administratora Systemu Informatycznego i Inspektora Ochrony Danych.
4.	Nieprzestrzeganie polityki czystego biurka oraz czystego ekranu.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Powiadomić Inspektora Ochrony Danych
5.	Wyniesienie kluczy od pomieszczeń biurowych poza budynek ZJO po zakończonej pracy.	Wezwać osobę popełniającą tę czynność, aby jej zaniechała. Powiadomić Inspektora Ochrony Danych

Załącznik nr 2a

Raport z naruszenia ochrony danych osobowych danych osobowych

Kod formy naruszenia ochrony danych ..... (wg tabeli)

1. Data ..... Godzina .....
2. Osoba powiadamiająca o zdarzeniu i inne osoby zaangażowane (imię, nazwisko, stanowisko):

.....

.....

3. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

.....

.....

4. Rodzaj zdarzenia i określenie okoliczności towarzyszących zdarzeniu oraz informacja o danych, które mogły zostać ujawnione:

.....

.....

.....

5. Podjęte działania:

.....

.....

6. Zabezpieczone materiały i dowody związane ze zdarzeniem:

.....

.....

7. Wstępna ocena przyczyn wystąpienia naruszenia:

.....

.....

8. Postępowanie wyjaśniające i naprawcze:

.....

.....

.....

(data i podpis Inspektora ochrony danych)

Inspektor Ochrony Danych
Zarząd Jednostek Oświatowych
- JB w Płocku
Tadeusz Borowicki

DYREKTOR
Zarządu Jednostek Oświatowych - JB
Maciej Krzemiński

Załącznik nr 2b

Raport z zagrożenia bezpieczeństwa danych osobowych

Kod formy zagrożenia ochrony danych ..... (wg tabeli)

1. Data ..... Godzina .....

2. Osoba powiadamiająca o zdarzeniu oraz inne osoby zaangażowane (imię, nazwisko, stanowisko):

.....

.....

3. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

.....

.....

4. Rodzaj zdarzenia i określenie okoliczności towarzyszących zdarzeniu oraz informacja o danych, które mogły zostać ujawnione:

.....

.....

.....

5. Podjęte działania:

.....

.....

6. Zabezpieczone materiały i dowody związane ze zdarzeniem:

.....

.....

7. Wstępna ocena przyczyn wystąpienia zagrożenia:

.....

.....

8. Postępowanie wyjaśniające i naprawcze:

.....

.....

.....

(data i podpis Inspektora ochrony danych)

Inspektor Ochrony Danych
Zarząd Jednostek Oświatowych
- JB w Płocku
Tadeusz Borowicki

DYREKTOR
Zarządu Jednostek Oświatowych - JB
Maciej Krzemiński

Załącznik nr 3

Rejestr zagrożeń i incydentów prowadzących do naruszeń ochrony danych osobowych

Lp.	Opis incydentu/zagrożenia	Osoba zgłaszająca	Podjęte działania zapobiegawcze i naprawcze	Skutki podjętych działań	Okres wystąpienia incydentu/zagrożenia	Uwagi dotyczące konieczności wysyłania zawiadomień

Inspektor Ochrony Danych
Zarząd Jednostek Oświatowych
- JB w Płocku
Tadeusz Borowicki

DYREKTOR
Zarządu Jednostek Oświatowych - JB
Maciej Krzemiński