BIURO BEZPIECZEŃSTWA INFORMCJI
URZĄD MIASTA W BYDGOSZCZY

Kodeks

postępowania w zakresie ochrony danych osobowych w publicznych placówkach oświatowych, dla których organem prowadzącym jest Miasto Bydgoszcz.

WERSJA 1.0

ZATWIERDZIŁ
DYREKTOR
BIURA BEZPIECZEŃSTWA INFORMACJI
URZĘDU MIASTA W BYDGOSZCZY

Marek STANIEWSKI

OPRACOWAŁ
INSPEKTOR
BIURA BEZPIECZEŃSTWA INFORMACJI
URZĘDU MIASTA W BYDGOSZCZY

Marek ŁUGIEWICZ

Bydgoszcz, wrzesień 2018 rok

Spis treści

I. Wstęp.

Podstawą do opracowania i wdrożenia niniejszego kodeksu postępowania jest Rozporządzenie Parlamentu Europejskiego i Rady 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 RODO).

Niniejszy Kodeks należy traktować jako minimalne i obowiązkowe wymagania, które publiczna placówka oświatowa powinna wdrożyć do działalności służbowej, aby funkcjonować w zgodności z przepisami wynikającymi z RODO.

Niniejszy „*Kodeks postępowania w zakresie ochrony danych osobowych w publicznych placówkach oświatowych, dla których organem prowadzącym jest Miasto Bydgoszcz*" zwanym w dalszej części Kodeksem, powstał w celu określenia zadań inspektora ochrony danych, dyrektora publicznej placówki oświatowej, który pełni rolę administratora danych osobowych, pracowników placówki oraz ustalenia wzajemnych relacji pomiędzy nimi.

Przyjęte reguły i zasady postępowania dotyczą wszystkich pracowników publicznych placówek oświatowych oraz wykonawców usług i dostaw, jak również inne podmioty współpracujące z tymi placówkami, które w ramach realizacji zawartych z nimi umów i na czas ich realizacji muszą uzyskać dostęp do danych. Przyjęte zasady obowiązują niezależnie od formy przetwarzania informacji.

II. Definicje.

Użytym w Kodeksie poniższym pojęciom nadaje się następujące znaczenie:

Administrator danych osobowych - właściwa publiczna placówka oświatowa, którą reprezentuje dyrektor.

Dane osobowe - wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Administrator Systemu Informatycznego (ASI) - pracownik lub wskazana przez dyrektora osoba fizyczna albo prawna, odpowiedzialny za wdrożenie i stosowanie zasad bezpieczeństwa danych osobowych w zakresie technicznych i organizacyjnych zabezpieczeń systemu informatycznego.

Przetwarzanie danych osobowych - rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Poufność – zapewnienie, że dane nie są udostępniane lub ujawniane nieautoryzowanym osobom lub podmiotom.

Integralność – zapewnienie, że dane nie zostały zmienione w sposób nieautoryzowany.

Dostępność – zapewnienie, że dane będą możliwe do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot.

Autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji).

Niezaprzeczalność – zapewnienie braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.

RODO – Rozporządzenie Parlamentu Europejskiego i Rady 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).

SKD – system kontroli dostępu (elektroniczny) do wyznaczonych pomieszczeń lub stref.

Pomieszczenia szczególne – pomieszczenia, w których głównie przetwarzane są dane osobowe oraz zdeponowana jest dokumentacja lub sprzęt komputerowy zawierające takie dane lub znajdują się w nich rejestratory monitoringu, a także centrale alarmowe (np. sekretariat, pomieszczenia dyrekcji, portiernia, pokój intendenta, gabinet pedagoga, gabinet higienistki, itp.).

Organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych (PUODO).

III. Zasady przetwarzania informacji.

1. **Zasada ograniczenia celu** – dane osobowe muszą być zbierana w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami. Cel ten musi być określony w momencie ich pozyskiwania. (art. 5 ust.1 lit. b RODO).

2. **Zasada zgodności z prawem, rzetelności i przejrzystości** – dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dotyczą. Wszelkie informacje i komunikaty związane z przetwarzaniem muszą być łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem (art. 5 ust. 1 lit. a i motyw 39 RODO).

3. **Zasada minimalizacji danych** - pozyskiwane mogą być jedynie dane adekwatne i niezbędne dla osiągnięcia celów konkretnych, uzasadnionych i określonych w momencie zbierania danych. Nie można zbierać danych osobowych, które nie mają związku z celem przetwarzania, są nadmiarowe lub już nieprzydatne (np. ze względu na ich nieaktualność) (art. 5 ust. 1 lit. c i motyw 39 RODO).

4. **Zasada prawidłowości danych** - dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Należy podejmować wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (art. 5 ust. 1 lit. d RODO).

5. **Zasada ograniczenia czasowego** - dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, dla których dane te są przetwarzane. Przechowywanie danych zgromadzonych, np. w celu realizacji umowy powinno być zakończone w momencie przedawnienia roszczeń czy innych praw i obowiązków wynikających z przepisów prawa (art. 5 ust. 1 lit. e RODO).

6. **Zasada integralności i poufności** - dane osobowe muszą być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (art. 5 ust. 1 lit. f RODO).

7. **Zasada ograniczonego przetwarzania -** podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, przez co rozumie się przetwarzanie na podstawie i w zakresie udzielonego upoważnienia lub zawartej umowy powierzenia przetwarzania danych osobowych. (art. 28 i 29 RODO)**.**

8. **Zasada rozliczalności –** wszelkie czynności i decyzje związane z ochroną danych osobowych muszą być dokumentowane. Działania związane z przetwarzaniem danych (w szczególności decyzje dotyczące zarządzania dostępem do informacji lub zasobów służących do jej przetwarzania) muszą być dokumentowane lub powodować tworzenie zapisów pozwalających na ocenę zgodności podejmowanych działań z przyjętymi zasadami.

9. **Zasada odpowiedzialności** – odpowiedzialność za czynności przetwarzania, podejmowanie decyzji o dostępie do informacji, dokumentację, procesy i środki przetwarzania musi być jednoznacznie przypisana do pracowników lub komórek organizacyjnych.

10. **Zasada wiedzy koniecznej** – możliwość uzyskania dostępu do informacji wyłącznie w zakresie i w ramach realizowanych obowiązków służbowych lub zapisów umowy.

11. **Zasada identyfikowalności** – osoby, procesy, urządzenia uzyskujące dostęp do informacji lub zasobów służących do jej przetwarzania muszą być w sposób jednoznaczny identyfikowalne.

12. **Zasada uwierzytelnienia** – mechanizmy kontroli dostępu osoby, procesu, urządzenia do informacji lub zasobów służących do jej przetwarzania muszą wykorzystywać właściwe środki uwierzytelniające oraz zapewniać bezpieczeństwo informacji uwierzytelniających.

13. **Rozdzielenie obowiązków** – rozdzielenie obowiązków związanych z podejmowaniem decyzji związanych z dostępem do informacji oraz zasobów wykorzystywanych do jej przetwarzania od obowiązków związanych z techniczną ich realizacją.

14. **Zasada uwzględnienia ochrony danych w fazie projektowania** – wdrożenie nowej czynności przetwarzania (w szczególności z wykorzystaniem narzędzi informatycznych) musi być poprzedzone fazą planowania obejmującą analizę związanych z nią ryzyk oraz uwzględnienie odpowiednich zabezpieczeń.

15. **Zasada domyślnej ochrony** - domyślnie przetwarzane mogą być wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.

IV. Zakres obowiązków dyrektora.

1. Administratorem danych osobowych jest właściwa publiczna placówka oświatowa, którą reprezentuje dyrektor.
2. Dyrektor publicznej placówki oświatowej zapewnia bezpieczeństwo przetwarzania informacji, ze szczególnym uwzględnieniem danych osobowych, poprzez zastosowanie środków technicznych i organizacyjnych adekwatnych do występujących ryzyk oraz kategorii danych objętych ochroną. W szczególności zapewnia środki i zasoby umożliwiające zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem i zniszczeniem.
3. Dyrektor publicznej placówki oświatowej odpowiedzialny jest za:
   1) aktualność przetwarzanych danych osobowych;
   2) aktualność upoważnień do przetwarzania danych osobowych posiadanych przez podległych mu pracowników oraz ich adekwatność do zajmowanych stanowisk;
   3) aktualność uprawnień do pracy w systemach informatycznych posiadanych przez podległych mu pracowników oraz ich adekwatność do zajmowanych stanowisk;
   4) aktualność rejestru czynności przetwarzania i kategorii czynności przetwarzania;
   5) wypełnianie obowiązku informacyjnego względem osób, których dane osobowe są przetwarzane;
   6) zbieranie stosownych zgód oraz prowadzenie rejestru tych zgód;
   7) przekazywanie danych osobowych do przetwarzania przez inny podmiot (innego administratora danych osobowych) na podstawie umowy powierzenia przetwarzania danych osobowych oraz prowadzenie rejestru takich umów;
   8) udostępnianie danych osobowych innym podmiotom, na ich wniosek, w celu realizacji ich celów i prowadzenie rejestru takich udostępnień;
   9) zarządzanie dostępem podległych pracowników do pomieszczeń placówki oświatowej;
   10) informowanie inspektora ochrony danych o nowych, planowanych czynnościach przetwarzania **w terminie nie krótszym niż 30 dni** przed planowaną datą rozpoczęcia przetwarzania;

11) wyznaczenie, administratora systemów informatycznych (ASI) odpowiedzialnego w szczególności za wdrażanie i utrzymanie zabezpieczeń technicznych i organizacyjnych systemów informatycznych, utrzymanie aktualnego rejestru tych systemów i określenie mu zakresu obowiązków;
12) zapoznanie podległych pracowników z zasadami dotyczącymi ochrony danych osobowych obowiązującymi w placówce oświatowej, w tym w szczególności z zasadami identyfikowania incydentów i naruszeń w zakresie ochrony danych osobowych oraz trybem ich zgłaszania;
13) **niezwłoczne** informowanie inspektora ochrony danych o przypadkach naruszeń danych osobowych, **nie później jednak niż do 24 godzin** od momentu ich stwierdzenia;
14) wskazanie i widoczne oznaczenie sprzętu komputerowego w placówce, który wykorzystywany będzie wyłącznie do celów dydaktycznych bez możliwości przetwarzania na nim danych osobowych (naklejka w kolorze zielonym) oraz na sprzęt wykorzystywany do przetwarzania danych osobowych (naklejka w kolorze czerwonym);
15) wyznaczenie, w porozumieniu z administratorem systemów informatycznych, miejsca depozytu sprzętu komputerowego pracowników (z naklejką w kolorze czerwonym), którzy nie będą z niego korzystać przez dłuższy okres (np.: wakacje, ferie, urlop, zwolnienie lekarskie, remonty, itp.), biorąc pod uwagę możliwy nadzór fizyczny nad zdeponowanym sprzętem (np.: sekretariat, portiernia, inne pomieszczenie dozorowane przez wskazaną osobę lub system alarmowy albo monitoring).

4. W sytuacjach szczególnych, wymagających odstępstwa od niniejszego kodeksu, decyzję o takim odstępstwie podejmuje dyrektor, jednocześnie informując o tym inspektora ochrony danych.

V. Zakres obowiązków inspektora ochrony danych.

1. Inspektor ochrony danych ma następujące zadania:
   1) informowanie dyrektora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie poprzez:
      a) opiniowanie dokumentów,
      b) konsultacje działań dyrektora w zakresie ochrony danych osobowych,
      c) udzielanie interpretacji przepisów dotyczących ochrony danych osobowych,
      d) udzielanie odpowiedzi na zgłoszone zapytania;
   2) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz postanowień niniejszego kodeksu postępowania, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   3) udzielanie na żądanie dyrektora zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
   4) pełnienie funkcji punktu kontaktowego dla:
      a) organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
      b) osób, których dane dotyczą, w zakresie przetwarzania ich danych osobowych oraz wykonywania praw im przysługujących na mocy przepisów RODO;
   5) nadzór nad rejestrami kategorii i czynności przetwarzania, prowadzonymi przez dyrektora, w tym zatwierdzanie czynności przetwarzania;
   6) obsługa incydentów i naruszeń dotyczących ochrony danych osobowych.

VI. Zasady współpracy inspektora ochrony danych z dyrektorem.

1. Do bieżącej komunikacji (zapytania, prośby o interpretację przepisów, konsultacje, itp.) pomiędzy dyrektorem a inspektorem ochrony danych, należy wykorzystywać wyłącznie pocztę elektroniczną: **iodoswiata@um.bydgoszcz.pl**
2. Dyrektor ma prawo wyznaczyć, spośród podległego mu personelu, swojego przedstawiciela do realizacji zadań organizacyjno – technicznych związanych z przestrzeganiem przepisów RODO. O wyznaczeniu lub zmianie swego przedstawiciela, dyrektor informuje inspektora ochrony danych.
3. Wyznaczenie przez dyrektora swego przedstawiciela do realizacji zadań organizacyjno – technicznych, nie znosi jego odpowiedzialności za przestrzeganie przepisów związanych z ochroną danych osobowych.
4. Wyznaczony przez dyrektora przedstawiciel ma prawo bezpośrednio kontaktować się z wyznaczonym inspektorem ochrony danych w sprawach dotyczących organizacyjno – technicznej ochrony danych osobowych.
5. W przypadku, gdy dyrektor nie zgadza się ze stanowiskiem inspektora ochrony danych zawartych w rekomendacjach po przeprowadzonym audycie, informuje o tym pisemnie Dyrektora Biura Bezpieczeństwa Informacji UM w Bydgoszczy, **w terminie 7 dni** od ich otrzymania.
6. Dyrektor, w szczególności, ma obowiązek zapewnić, by inspektor ochrony danych był informowany o wszystkich sprawach dotyczących ochrony danych osobowych.
7. Dyrektor wspiera inspektora ochrony danych w wypełnianiu przez niego zadań, zapewniając mu warunki i środki niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania.
8. Dyrektor zapewnia, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań.
9. Inspektor ochrony danych udziela dyrektorowi wszelkiej, niezbędnej pomocy merytorycznej w zakresie ochrony danych osobowych w postaci wskazówek, sugestii lub rekomendacji. Nie oznacza to jednak wykonywania za dyrektora spoczywających na nim zadań, w tym w szczególności opracowywania niezbędnej dokumentacji.
10. Tryb zgłaszania naruszeń i incydentów związanych z ochroną danych osobowych został szczegółowo określony w rozdziale X.

VII. Zakres obowiązków administratora systemów informatycznych (ASI).

1. Administrator systemów informatycznych realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym prowadzonym w publicznej placówce oświatowej, w szczególności wdraża, monitoruje i nadzoruje systemem informatyczny, w którym przetwarzane są dane osobowe poprzez;
   1) prowadzenie ewidencji:
      a) sprzętu komputerowego w placówce z podziałem na sprzęt wykorzystywany wyłącznie do celów dydaktycznych bez przetwarzania na nim danych osobowych (z naklejką w kolorze zielonym) oraz na sprzęt wykorzystywany do przechowywania i przetwarzania danych osobowych (z naklejką w kolorze czerwonym),
      b) urządzeń i połączeń sieci informatycznej,
      c) wykorzystywanych aplikacji,
      d) incydentów w systemie informatycznym, a także problemów i awarii w tych systemach;
   2) bieżące utrzymanie urządzeń i aplikacji obejmujące w szczególności:
      a) instalowanie i konfigurację sprzętu komputerowego, urządzeń sieciowych oraz aplikacji,
      b) instalowanie, aktualizację oraz monitorowanie działania systemów antywirusowych, których celem jest ochrona przed szkodliwym oprogramowaniem;
      c) instalowanie i konfigurację mechanizmów szyfrowania dysków,
      d) wykonywanie kopii zapasowych oraz okresowych weryfikacji pod kątem dalszej ich przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
      e) usuwanie z komputerów służbowych nieautoryzowanego oprogramowania bez konieczności uzyskania akceptacji użytkowników dla tego działania,
      f) gromadzenie i przechowywanie dzienników zdarzeń (logów),
      g) oznaczanie, w widoczny sposób za pomocą naklejek we właściwych kolorach, wskazany przez dyrektora sprzęt komputerowy,

h) wykonywanie i koordynację wykonywania napraw, konserwacji oraz likwidacji urządzeń komputerowych, na których zapisane są dane osobowe,

i) podejmowanie działania służących zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej, a także bezpiecznej teletransmisji;

3) zarządzanie dostępem do systemów informatycznych obejmujące w szczególności:

a) wdrożenie, aktualizację i nadzór nad działaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych,

b) przydzielanie każdemu użytkownikowi, na polecenie dyrektora, loginu oraz hasła do systemu informatycznego oraz dokonywanie ewentualnych modyfikacji uprawnień, a także dezaktywowanie kont użytkowników;

2. W przypadku stwierdzenia naruszenia zabezpieczeń systemu informatycznego, informuje dyrektora o zaistniałym naruszeniu i współpracuje z nim przy usuwaniu skutków naruszenia.
3. Monitoruje proces oddawania przez pracowników do depozytu sprzętu komputerowego (z naklejką w kolorze czerwonym), który nie będzie wykorzystywany przez dłuższy okres (np.: wakacje, ferie, urlop, zwolnienie lekarskie, remonty, itp.), biorąc pod uwagę możliwy nadzór fizyczny nad zdeponowanym sprzętem (np.: sekretariat, portiernia, inne pomieszczenie dozorowane przez wskazaną osobę lub system alarmowy albo monitoring).

VIII. Odpowiedzialność pracowników.

1. Każdy pracownik zobowiązany jest do:
   1) przestrzegania zasad niniejszego kodeksu oraz wydanych w tym zakresie zarządzeń dyrektora;
   2) bezpiecznego przetwarzania i ochrony danych osobowych, do których został upoważniony;
   3) **niezwłocznego** informowania dyrektora o przypadkach naruszeń danych osobowych, **nie później jednak niż do 3 godzin** od momentu ich stwierdzenia;
   4) zgłaszania do ASI oraz do dyrektora wszelkiego rodzaju odstępstw w działaniu systemu (np. spowolnienie pracy komputera, próby wymuszania haseł, komunikaty programów antywirusowych, itp.);
   5) zachowania poufności informacji z zakresu danych osobowych oraz wprowadzonych w placówce systemów ich zabezpieczeń;
   6) dbania o własny stan wiedzy z zakresu ochrony danych osobowych poprzez systematyczne samokształcenie;
   7) zdania do depozytu, wskazanego przez dyrektora, posiadanego sprzętu komputerowego (z naklejką w kolorze czerwonym), w przypadku przewidywanego nie korzystania z niego przez dłuższy okres (np.: wakacje, ferie, urlop, zwolnienie lekarskie, remonty, itp.).
4. Każdy pracownik odpowiedzialny jest za wszelkie czynności wykonane w systemach teleinformatycznych przy użyciu przypisanego do niego identyfikatora.
5. W stosunku do osób naruszających postanowienia niniejszego kodeksu wszczynane będzie postępowanie dyscyplinarne zgodnie z regulaminem pracy, obowiązującym w danej placówce oświatowej.
6. Wszczęcie postępowania dyscyplinarnego nie wyklucza odpowiedzialności karnej za przestępstwa popełnione przeciwko bezpieczeństwu informacji.

IX. Podstawowe zasady w zakresie bezpieczeństwa ochrony danych osobowych.

W celu zminimalizowania ryzyka związanego z naruszeniem ochrony danych osobowych, dyrektor oraz każdy pracownik publicznej placówki oświatowej powinien w szczególności, stosować niżej wskazane zasady związane z bezpieczeństwem osobowym, fizycznym i informatycznym.

1. Bezpieczeństwo osobowe:

1) każdy podległy pracownik posiada upoważnienie dyrektora do przetwarzania danych osobowych w zakresie odpowiednim dla jego stanowiska;
2) prowadzony jest rejestr wydanych upoważnień do przetwarzania danych osobowych;
3) prowadzona jest ewidencja szkolenia z zakresu ochrony danych osobowych;
4) każdy nowoprzyjęty pracownik publicznej placówki oświatowej, w okresie nie dłuższym niż trzy miesiące od chwili zatrudnienia, zobowiązany jest do odbycia szkolenia z zakresu ochrony danych osobowych, prowadzonego przez inspektora ochrony danych;
5) każdy podległy pracownik przechodzi szkolenie z zakresu ochrony danych osobowych, nie rzadziej niż raz na trzy lata;
6) każdy podległy pracownik zobowiązany został do zachowania poufności w zakresie posiadanych informacji dotyczących danych osobowych i systemów ich zabezpieczeń.

2. Bezpieczeństwo fizyczne:

1) przy zastosowaniu monitoringu wszystkie strefy monitorowane powinny zostać odpowiednio oznakowane, a fakt wprowadzenia monitoringu powinien zostać właściwie udokumentowany i przeprowadzony;
2) kluczami lub kartami (kodami) do pomieszczeń szczególnych powinny dysponować tylko osoby pisemnie upoważnione przez dyrektora;
3) pracownicy zdają, do depozytu wskazanego przez dyrektora, posiadany sprzęt komputerowy (z naklejką w kolorze czerwonym), na okres dłuższej,

przewidywanej nieobecności w pracy lub na czas trwania remontu pomieszczeń (np.: wakacje, ferie, urlop, zwolnienie lekarskie, itp.);

4) po zakończeniu pracy, pomieszczenia szczególne, powinny być pozamykane i właściwie zabezpieczone (np. załączenie SKD, włączenie alarmu, zdeponowanie kluczy) przed dostępem osób nieuprawnionych;
5) po zakończeniu pracy wszystkie okna w pomieszczeniach powinny zostać pozamykane oraz wyłączone z gniazdek te odbiorniki prądu elektrycznego, które mogą stanowić zwiększone ryzyko powstania pożaru (np. grzejniki elektryczne, ładowarki, czajniki, itp.);
6) po zakończeniu pracy w danym dniu, a także w przypadku opuszczenia miejsca pracy na dłuższy okres, należy umieszczać w szafach zamykanych na klucz, wszystkie dokumenty zawierające dane osobowe, tak aby dostęp do nich był utrudniony;
7) w przypadku wynoszenia poza placówkę, po zakończonej pracy, ze sobą kluczy lub kart dostępu do SKD, nadzór nad nimi powinien być szczególny, tak aby uniknąć ich kradzieży lub nieuprawnionego kopiowania;
8) należy tak urządzać pomieszczenia, w których przetwarza się dane osobowe, aby uniemożliwić dostęp osób postronnych do dokumentacji i informacji wyświetlanych na monitorach. Dotyczy to również pomieszczeń usytuowanych na parterze z dostępem przez okno do strefy ogólnodostępnej. W takim przypadku należy stosować na okna matowe folie okienne, tak aby ograniczyć możliwość wglądu do pomieszczenia z zewnątrz;
9) przyjmowanie interesantów w pomieszczeniach, w których przetwarzane są dane osobowe powinno odbywać się z zachowaniem szczególnej ostrożności z uwagi na możliwą utratę dokumentów. W tym celu należy stosować, w miarę możliwości, oddzielne stoliki (biurka) dla interesantów z możliwością wypełniania tam stosownych dokumentów;
10) w pomieszczeniach szczególnych, w których przetwarzane są dane osobowe, sprzątanie powinno odbywać się w godzinach pracy, pod nadzorem użytkownika pomieszczenia;
11) stosowane systemy alarmowe powinny być sprawne i włączane po zakończeniu pracy w danej strefie alarmu;

12) w przypadku nie posiadania umowy z firmą zewnętrzną, należy dokonywać cyklicznego sprawdzenia poprawności działania systemów alarmowych (raz w miesiącu), a wyniki sprawdzenia odnotowywać w „Dzienniku sprawdzeń poprawności działania systemu alarmowego”;
13) do bieżącej obsługi systemu alarmowego należy wyznaczyć odpowiedzialnego pracownika placówki lub powierzyć te zadania wyspecjalizowanej firmie;
14) dokumentację niepodlegającą archiwizacji i zawierającą dane osobowe należy niszczyć wyłącznie w niszczarce do dokumentów;
15) ze względu na przetwarzanie szczególnych danych osobowych przez pedagoga szkolnego, jego dokumentacja oraz sprzęt komputerowy objęty jest szczególnym nadzorem ze strony dyrektora oraz ASI.

3. Bezpieczeństwo informatyczne:

1) wyznaczenie przez dyrektora administratora systemów informatycznych (ASI);
2) każdy komputer jest oznakowany w widoczny sposób za pomocą naklejki w kolorze zielonym – komputery, na których nie przechowuje się danych osobowych (komputery w salach dydaktycznych, które służą jedynie do logowania się w systemie VULCAN, jako urządzenia do tablic interaktywnych, itp.) albo w kolorze czerwonym – komputery, na których przechowuje się i przetwarza dane osobowe;
3) dotyczy sprzętu komputerowego przeznaczonego do przechowywania i przetwarzania danych osobowych (z czerwoną naklejką) (np. pedagoga szkolnego, intendenta, sekretarki, dyrektora, itp.):
   a) każdy sprzęt komputerowy przeznaczony do przechowywania i przetwarzania danych osobowych (z naklejką w kolorze czerwonym) jest przydzielony do konkretnego, głównego użytkownika, który odpowiada za niego również materialnie,
   b) dostęp do systemów informatycznych wymaga posługiwania się unikalnym, przypisanym w sposób jednoznaczny użytkownikowi loginem i hasłem,

c) zabronione jest użyczanie komukolwiek własnych loginów i haseł, jak również zabronione jest korzystanie z cudzego loginu i hasła w celu uzyskania dostępu do systemów informatycznych,
d) sprzęt komputerowy, w tym drukarki z zapisem danych, oddawany do serwisu powinien, w miarę możliwości, być oddawany bez dysku twardego zawierającego dane osobowe, a jeżeli jest to niemożliwe, powinien być oddawany na podstawie umowy przetwarzania danych osobowych wraz z zobowiązaniem serwisu do zachowania poufności,
e) zabronione jest przekazywanie komputerów służbowych i innych nośników danych osobom nieuprawnionym,
f) niedopuszczalne jest, aby dwóch lub większa liczba pracowników wykorzystywała wspólnie jedno, imienne konto użytkownika,
g) czynności wykonywane przez użytkowników systemów teleinformatycznych powinny być rejestrowane i archiwizowane (systemowe dzienniki zdarzeń),
h) hasło przydzielone pracownikowi przez ASI musi zostać zmienione na własne, po pierwszym udanym zalogowaniu,
i) stosuje się szyfrowanie dysków;

4) dopuszcza się, aby komputery w salach dydaktycznych posiadały login i hasło przypisane do sprzętu i znane tylko pracownikom wykorzystującym je do celów dydaktycznych;
5) każdy komputer służbowy powinien być wyposażony w aktualny program antywirusowy monitorujący bezpieczeństwo wszystkich przetwarzanych plików;
6) instalowanie oprogramowania na komputerach służbowych możliwe jest wyłącznie przez ASI;
7) w przypadku wykorzystania przenośnych urządzeń komputerowych w miejscach publicznych nie korzystać z otwartych i niezabezpieczonych sieci WIFI, aby uniknąć przejęcia zasobów przez nieupoważnione osoby;
8) przenośne urządzenia komputerowe powinny być fizycznie chronione przed kradzieżą, szczególnie, kiedy są pozostawione w bagażniku samochodu lub innym środku transportu, pokoju hotelowym, centrum konferencyjnym lub miejscu spotkań, itp.;

9) urządzenia informatyczne i nośniki danych przenoszące dane osobowe, nie powinny być pozostawiane bez opieki. O ile to możliwe powinny być fizycznie blokowane lub zamykane (dotyczy to komputerów, notebooków, telefonów komórkowych, pendrive'ow, kart typu flash, płyt CD, DVD, itp.);
10) użytkownicy przekazujący dane osobowe poza teren placówki oświatowej przy użyciu nośników informatycznych, zobowiązani są do zaszyfrowania przekazywanych informacji i zabezpieczenia danych hasłem. Hasło powinno być przekazane odbiorcy danych innym kanałem komunikacyjnym niż nośnik danych (np. zaszyfrowany plik wysyłany jest pocztą elektroniczną a hasło, np. SMS'em);
11) strony internetowe powinny być zaopatrzone w widoczną politykę prywatności oraz politykę zbierania coockies (jeżeli jest wprowadzona taka możliwość zbierania danych);
12) służbowe skrzynki pocztowe pracowników mogą być monitorowane przez dyrektora, stosownie do art. 223 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2018 r. poz. 917, z późn. zm.), a pracownicy z którymi rozwiązano stosunek pracy, powinny utracić możliwość z ich korzystania;
13) każdy użytkownik systemów informatycznych zobowiązany jest do zgłaszania ASI wszelkiego rodzaju odstępstw w działaniu systemu (np. spowolnienie pracy komputera, próby wymuszania haseł, komunikaty programów antywirusowych, itp.);
14) komputery będące własnością placówki oświatowej mogą być wykorzystywane wyłącznie do celów służbowych;
15) dopuszcza się przetwarzanie danych osobowych na prywatnych urządzeniach (komputerach, notebookach) tylko wtedy, gdy jest to niezbędne i uzasadnione. W tym przypadku należy ograniczyć dostęp do danych osobowych członkom rodziny i osobom postronnym poprzez założenie oddzielnych kont użytkowników zaopatrzonych hasłem, szyfrowanie dostępu do dysku, szyfrowanie poczty, itp. Przed dopuszczeniem do przetwarzania danych osobowych na prywatnym urządzeniu, dyrektor odbiera pisemne oświadczenie o zapoznaniu się pracownika z zasadami przetwarzania danych osobowych obowiązującym w niniejszym kodeksie oraz w placówce oświatowej;

16) przetwarzane dane osobowe powinny znajdować się wyłącznie na komputerach i innych urządzeniach, nad którymi użytkownik ma pełną kontrolę. Zabrania się przekazywania danych osobowych na dalsze serwery, zapisywanie w chmurze, na hostingi, itp.;
17) dopuszcza się przesyłanie służbowych dokumentów zawierających dane osobowe z prywatnych skrzynek pocztowych, przy zastosowaniu szyfrowania poczty oraz ograniczenia dostępu do konta poczty dla osób postronnych.
18) należy zobowiązać pracowników, którzy kończą pracę i którzy przetwarzali dane osobowe na komputerach prywatnych lub innych urządzeniach, do niezwłocznego usunięcia danych z tych komputerów lub urządzeń. Stosować w takim przypadku oświadczenia pracowników i uzależnić podpisanie karty obiegowej pracownika od złożenia takiego oświadczenia;
19) zabronione jest przechowywanie i przetwarzanie prywatnych dokumentów oraz wiadomości elektronicznych na komputerach służbowych;

X. Zasady postępowania w przypadku wystąpienia incydentów lub naruszeń.

1. Zgłaszanie naruszeń i incydentów związanych z ochroną danych osobowych należy realizować w relacji „Pracownik placówki ⟶ Dyrektor placówki ⟶ Inspektor ochrony danych ⟶ Dyrektor placówki ⟶ Prezes Urzędu Ochrony Danych Osobowych”.
1. Zgłoszenie przez pracownika placówki naruszenia lub incydentu do dyrektora, w trybie o którym mowa w pkt. 1, należy realizować **niezwłocznie**, **nie później jednak niż do 3 godzin** od momentu jego stwierdzenia.
2. Zgłoszenie przez dyrektora naruszenia lub incydentu do inspektora ochrony danych, w trybie o którym mowa w pkt. 1, należy realizować **niezwłocznie**, **nie później jednak niż do 24 godzin** od momentu jego stwierdzenia.
3. Ostateczną decyzję o zakwalifikowaniu zdarzenia do kategorii naruszeń i zgłoszeniu do PUODO podejmuje dyrektor, po uprzedniej konsultacji z inspektorem ochrony danych.
4. W przypadku stwierdzenia przesłanki do wystąpienia naruszenia praw i wolności osób fizycznych, dyrektor powinien:
   1) zastosować wszelkie możliwe środki w celu zminimalizowania ewentualnych negatywnych skutków;
   2) dokonać analizy w kontekście wstępnego zakwalifikowania zdarzenia do kategorii incydentów albo naruszeń;
   3) skonsultować się **w trybie pilnym** (do 24 godzin), wszelkimi możliwymi środkami komunikacji, z inspektorem ochrony danych;
   4) wypełnić w systemie informatycznym zgłoszenie naruszenia i przesłać go do inspektora ochrony danych;
   5) zarejestrować zdarzenie w rejestrze naruszeń ochrony danych;
   6) zapoznać się z opinią i rekomendacjami inspektora ochrony danych;
   7) w przypadku zakwalifikowania zdarzenia do kategorii **naruszeń o niskim ryzyku naruszenia praw i wolności osób fizycznych (incydentu)**, podjąć działania opisane w pkt. 5 ppkt 1-6 oraz dodatkowo podjąć działania naprawcze rekomendowane przez inspektora ochrony danych;

8) w przypadku zakwalifikowania zdarzenia do kategorii **naruszeń o średnim ryzyku naruszenia praw i wolności osób fizycznych**, podjąć działania opisane w pkt. 5 ppkt 1-6 oraz dodatkowo:
   a) po konsultacji z inspektorem ochrony danych wypełnić stosowny formularz i zgłosić naruszenie do Prezesa Urzędu Ochrony Danych Osobowych, **nie później niż do 72 godzin** od momentu stwierdzenia naruszenia,
   b) podjąć działania naprawcze rekomendowane przez inspektora ochrony danych;
9) w przypadku zakwalifikowania zdarzenia do kategorii **naruszeń o wysokim ryzyku naruszenia praw i wolności osób fizycznych**, podjąć działania opisane w pkt. 5 ppkt 1-6 oraz dodatkowo:
   a) po konsultacji z inspektorem ochrony danych wypełnić stosowny formularz i zgłosić naruszenie do Prezesa Urzędu Ochrony Danych Osobowych, **nie później niż do 72 godzin** od momentu stwierdzenia naruszenia,
   b) dokonać analizy przypadku w kontekście art. 34 ust. 3 RODO i ewentualnie powiadomić niezwłocznie osoby, których dane dotyczą, o takim naruszeniu,
   c) podjąć działania naprawcze rekomendowane przez inspektora ochrony danych.

5. Po zakończeniu procesu zgłoszenia incydentu lub naruszenia, dyrektor dokonuje analizy wystąpienia nieprawidłowości, ustala winnych zaistniałej sytuacji oraz przeprowadza stosowne postępowanie dyscyplinarne.

XI. Zasady uruchomienia monitoringu wizyjnego.

1. Podstawa prawna:
   1) art. 22^2 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy (Dz. U. z 2018 r. poz. 917, z późn. zm.);
   2) art. 108a ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2018 r. poz. 996, z późn. zm.).
2. Jeżeli jest to niezbędne do zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony mienia dyrektor szkoły lub placówki może wprowadzić szczególny nadzór nad pomieszczeniami szkoły lub placówki lub terenem wokół szkoły lub placówki w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring).
3. W tym celu dyrektor szkoły lub placówki:
   1) uzgadnia z organem prowadzącym szkołę lub placówkę:
      a) konieczność wprowadzenia monitoringu,
      b) odpowiednie środki techniczne i organizacyjne w celu ochrony przechowywanych nagrań obrazu oraz danych osobowych uczniów, pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, uzyskanych w wyniku monitoringu;
   2) przeprowadza konsultacje:
      a) z radą pedagogiczną,
      c) radą rodziców,
      d) samorządem uczniowskim;
   3) informuje uczniów i pracowników szkoły lub placówki o wprowadzeniu monitoringu, w sposób przyjęty w danej szkole lub placówce, nie później niż 14 dni przed uruchomieniem monitoringu;
   4) oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż dzień przed jego uruchomieniem;
   5) przed dopuszczeniem osoby do wykonywania obowiązków służbowych informuje ją na piśmie o stosowaniu monitoringu.