BIURO BEZPIECZEŃSTWA INFORMACJI
URZĄD MIASTA W BYDGOSZCZY

Kodeks postępowania

w zakresie ochrony danych osobowych

w publicznych placówkach oświatowych,

dla których organem prowadzącym

jest Miasto Bydgoszcz.

§ 1
WSTĘP

Podstawą do opracowania i wdrożenia niniejszego **„Kodeksu postępowania w zakresie ochrony danych osobowych w publicznych placówkach oświatowych, dla których organem prowadzącym jest Miasto Bydgoszcz", zwanego dalej „Kodeksem"** 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" 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.

§ 2
DEFINICJE

Administrator Danych Osobowych (ADO), zwany dalej Administratorem – właściwa publiczna placówka oświatowa, którą reprezentuje Dyrektor.

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 4 maja 2016 r.).

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.

Dane osobowe - oznaczają 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;.

Przetwarzanie danych osobowych – oznacza 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.

Zgoda osoby, której dane dotyczą – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;

Podmiot przetwarzający oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi / podmiotowi przetwarzającemu / pracownikom w zakresie obowiązującego prawa o ochronie danych i tej polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Pseudonimizacja – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

Szczególne kategorie danych osobowych (dane wrażliwe) – oznaczają dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

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;

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

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.).

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

§ 3
ZAKRES STOSOWANIA

1. „Kodeks" odnosi się do danych osobowych przetwarzanych w sposób tradycyjny w formie papierowej jak i elektronicznej.
2. W celu ochrony interesów osób, których dane dotyczą, dokłada się szczególnej staranności w zakresie przetwarzania danych osobowych, w szczególności poprzez:
   1) przetwarzanie danych osobowych zgodnie z przepisami prawa;
   2) zbieranie danych osobowych dla oznaczonych i zgodnych z prawem celów, oraz nie poddawanie danych osobowych przetwarzaniu niezgodnie z tymi celami;
   3) poprawność merytoryczną danych osobowych i adekwatność danych osobowych z celem, z którym są przetwarzane;
   4) przechowywanie danych osobowych w sposób umożliwiający identyfikację osób, których dane osobowe dotyczą przez okres nie dłuższy, niż jest to niezbędne do osiągnięcia celu w jakim dane te zostały udostępnione.
3. 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.

§ 4
ZADANIA ADMINISTRATORA DANYCH OSOBOWYCH (DYREKTORA PLACÓWKI)

Administratorem Danych Osobowych jest właściwa publiczna placówka oświatowa, którą reprezentuje Dyrektor. 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, zbieraniem przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem i zniszczeniem.

1. 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) prowadzenie przy współpracy z IOD rejestru czynności przetwarzania i kategorii czynności przetwarzania (w tym ich aktualizacji);

   5) przestrzeganie zapisów art. 13 i 14 RODO – czyli realizację obowiązku informacyjnego względem osób, których dane osobowe są przetwarzane;

   6) w sytuacji, gdy brak jest przepisu prawa, stworzenie przy współpracy z IOD formularza zgód oraz prowadzenie rejestru tych zgód;

   7) stosowanie umowy powierzenia przetwarzania danych osobowych w momencie przekazania danych osobowych innym podmiotom mającym realizować cel ADO;

   8) udostępnianie danych osobowych innym podmiotom, na ich wniosek, w celu realizacji ich celów i prowadzenie rejestru takich udostępnień;

   9) informowanie Inspektora Ochrony Danych o nowych, planowanych czynnościach przetwarzania **w terminie nie krótszym niż 30 dni** przed planowaną datą rozpoczęcia przetwarzania;

   10) 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. W przypadku braku możliwości wyznaczenia ASI wewnątrz publicznej placówki oświatowej podjęcie współpracy z firmą informatyczną w ramach obsługi publicznej placówki oświatowej w zakresie zabezpieczenia przetwarzania w/w danych w systemach informatycznych;

   11) 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 (szkolenia, dokumentacja obowiązująca w publicznej placówce oświatowej);

   12) zarządzanie dostępem podległych pracowników do pomieszczeń placówki oświatowej;

   13) dokonywanie przeglądu danych osobowych dla potrzeb zakładowego funduszu świadczeń socjalnych nie rzadziej niż raz w roku kalendarzowym w celu ustalenia niezbędności

ich dalszego przechowywania oraz sporządzanie z tego procesu protokołu lub notatki służbowej;

14) odpowiedzialność za przechowywanie dokumentów z danymi osobowymi zgodnie z przepisami prawa i instrukcją kancelaryjną / jednolitym rzeczowym wykazem akt, zatwierdzonym przez Archiwum Państwowe oddział w Bydgoszczy;

15) **niezwłoczne** informowanie Inspektora Ochrony Danych o przypadkach naruszeń danych osobowych, **nie później jednak niż do 24 godzin** od momentu ich stwierdzenia.

2. W sytuacjach szczególnych, wymagających odstępstwa od niniejszego „Kodeksu", decyzję o takim odstępstwie podejmuje Dyrektor, jednocześnie informując o tym Inspektora Ochrony Danych Osobowych.

§ 5
ZADANIA INSPEKTORA OCHRONY DANYCH

Zgodnie z art. 39 RODO Inspektor Ochrony Danych realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1) informuje Aadministratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2) monitoruje przestrzeganie rozporządzenia RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk Aadministratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3) udziela na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
4) współpracuje z organem nadzorczym;
5) pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
6) sporządza projekty umów w zakresie powierzenia danych osobowych przetwarzającym; przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnionych do przetwarzania danych osobowych, w tym tematyka szkoleń obejmuje m.in.:

a) przepisy i procedury dotyczące ochrony danych osobowych, sporządzania i przechowywania kopii, niszczenia wydruków i zapisów na nośnikach;
b) sposoby ochrony danych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą;

c) obowiązki osób upoważnionych do przetwarzania danych osobowych;
d) odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych;
e) zasady i procedury określone w „Kodeksie".

§ 6
ZADANIA ADMINISTRATORA SYSTEMU INFORMATYCZNEGO (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 oraz na sprzęt wykorzystywany do przechowywania i przetwarzania danych osobowych;
      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, na którym przetwarzane są dane osobowe a 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).

§ 7
ZASADY WSPÓŁPRACY INSPEKTORA OCHRONY DANYCH Z DYREKTOREM

1. Do bieżącej komunikacji (zapytania, prośby o interpretację przepisów, konsultacje, itp.) pomiędzy Dyrektorem a Inspektorem Ochrony Danych, a także pracownikami a IOD - 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 publicznej placówki oświatowej, 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.

§ 8
OBOWIĄZKI OSOBY UPOWAŻNIONEJ (PRACOWNIKA) DO PRZETWARZANIA DANYCH OSOBOWYCH

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana:

1) przetwarzać dane osobowe wyłącznie w zakresie ustalonym w upoważnieniu przez Administratora Danych Osobowych i tylko w celu wykonywania nałożonych na nią obowiązków. Rozwiązanie stosunku pracy oraz odwołanie z pełnionej funkcji/stanowiska powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;
2) zachować w tajemnicy dane osobowe oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u Administratora Danych Osobowych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;
3) stosować się do przepisów prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszego „Kodeksu" w zakresie ochrony danych osobowych, a także procedur oraz wytycznych mających na celu zgodne z prawem przetwarzanie danych osobowych;
4) korzystać z systemu informatycznego w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi;
5) zabezpieczać dane osobowe przed ich udostępnieniem osobom nieupoważnionym;
6) **niezwłocznie informować ADO o przypadkach naruszeń danych osobowych, nie później jednak niż do 3 godzin od momentu ich stwierdzenia;**
7) zgłaszania do ASI oraz do Dyrektora wszelkiego rodzaju odstępstw w działaniu systemu (np. spowolnienie pracy komputera, próby wymuszania haseł, komunikaty programów antywirusowych, itp.);
8) zdania do depozytu, wskazanego przez Dyrektora, posiadanego sprzętu komputerowego, w przypadku przewidywanego niekorzystania z niego przez dłuższy okres (np.: wakacje, ferie, urlop, zwolnienie lekarskie, remonty, itp.).

§ 9
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 pięć lat**;
6) Każdy podległy pracownik oświadcza pisemnie o zachowaniu poufności w zakresie posiadanych informacji dotyczących danych osobowych i systemów ich zabezpieczeń.

§ 10
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 i wyznaczone przez Dyrektora;
3) Pracownicy zdają, do depozytu wskazanego przez Dyrektora, posiadany służbowy sprzęt komputerowy), 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 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;
6) 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;

7) 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;
8) Do bieżącej obsługi systemu alarmowego (antywłamaniowego) należy wyznaczyć odpowiedzialnego pracownika placówki lub powierzyć te zadania wyspecjalizowanej firmie;
9) Dokumentację niepodlegającą archiwizacji i zawierającą dane osobowe należy niszczyć wyłącznie w niszczarce do dokumentów;
10) Ze względu na przetwarzanie szczególnych danych osobowych przez pedagoga szkolnego, jego dokumentacja oraz sprzęt komputerowy objęty jest szczególnym nadzorem ze strony Dyrektora przy współpracy z ASI.

§ 11
BEZPIECZEŃSTWO INFORMATYCZNE

1) Wyznaczenie przez Dyrektora Administratora Systemów Informatycznych (ASI);
2) Dostęp do systemów informatycznych wymaga posługiwania się unikalnym, przypisanym w sposób jednoznaczny użytkownikowi loginem i hasłem;
3) 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;
4) Sprzęt komputerowy, w tym drukarki z zapisem danych, 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;
5) Zabronione jest przekazywanie komputerów służbowych i innych nośników danych osobom nieuprawnionym;
6) Niedopuszczalne jest, aby dwóch lub większa liczba pracowników wykorzystywała wspólnie jedno, imienne konto użytkownika;
7) Hasło przydzielone pracownikowi przez ASI musi zostać zmienione na własne, po pierwszym udanym zalogowaniu;
8) Stosuje się szyfrowanie dysków;
9) Dopuszcza się, aby komputery w salach dydaktycznych posiadały login i hasło przypisane do sprzętu i znane tylko pracownikom wykorzystującym je do celów dydaktycznych;
10) Każdy komputer służbowy powinien być wyposażony w aktualny program antywirusowy monitorujący bezpieczeństwo wszystkich przetwarzanych plików;

11) Instalowanie oprogramowania na komputerach służbowych możliwe jest wyłącznie przez ASI lub firmę informatyczna;
12) W przypadku wykorzystania przenośnych urządzeń komputerowych w miejscach publicznych nie korzystać z otwartych i niezabezpieczonych sieci WIFI, aby uniknąć przejęcia zasobów przez nieupoważnione osoby;
13) 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.;
14) 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.);
15) 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);
16) Urządzenia informatyczne i nośniki danych przenoszące dane osobowe muszą być zaszyfrowane / zabezpieczone hasłem;
17) Strony internetowe powinny być zaopatrzone w widoczną politykę prywatności oraz politykę zbierania coockies (jeżeli jest wprowadzona taka możliwość zbierania danych);
18) W przypadku możliwości napisania e-mail do publicznej placówki oświatowej przy użyciu jej strony internetowej pod formularzem powinna znaleźć się informacja o wyrażeniu zgody na przetwarzanie danych osobowych (adres e-mail wnioskodawcy) oraz klauzula informacyjna zgodna z art. 13 RODO;
19) Każdy użytkownik systemów informatycznych zobowiązany jest do zgłaszania ASI oraz informowania Dyrektora publicznej placówki oświatowej wszelkiego rodzaju odstępstw w działaniu systemu (np. spowolnienie pracy komputera, próby wymuszania haseł, komunikaty programów antywirusowych, itp.);
20) Komputery będące własnością placówki oświatowej mogą być wykorzystywane wyłącznie do celów służbowych;
21) 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 przetwarzanych danych osobowych uczniów, 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 obowiązujących w niniejszym „Kodeksie" oraz w placówce oświatowej;**

22) Nie rekomenduje się przekazywania danych osobowych na dalsze serwery, zapisywanie w chmurze, na hostingi, itp.. Jeżeli publiczna placówka oświatowa chce korzystać z tzw. „chmury" jest zobowiązania do: podpisania umowy powierzenia danych osobowych zgodnie z art. 28 RODO z firmą dostarczającą w/w aplikację, wyznaczenia osoby odpowiedzialnej za udostępniane informacje uczniom i rodzicom oraz pozostałym nauczycielom i pracownikom danej placówki oświatowej, wyznaczenia osoby odpowiedzialnej za kontrolę nad tworzonymi kontami użytkowników chmury czy innej aplikacji służącej do celów dydaktycznych;

23) Dopuszcza się przesyłanie służbowych dokumentów zawierających dane osobowe z prywatnych skrzynek pocztowych, przy zastosowaniu szyfrowania poczty oraz uniemożliwieniu dostępu do konta poczty dla osób postronnych;

24) Należy zobowiązać pracowników, którzy kończą pracę i którzy przetwarzali dane osobowe na komputerach prywatnych lub innych urządzeniach przenośnych, do niezwłocznego usunięcia danych z tych komputerów lub urządzeń. Stosować w takim przypadku oświadczenia pracowników.

§ 12
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;
      e) zakładową organizacją związkową lub przedstawicielem pracowników (jeśli zachodzi taka konieczność);

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.

§ 13
ODPOWIEDZIALNOŚĆ OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Niezastosowanie się do „Kodeksu", którego założenia określa niniejszy dokument, i naruszenie procedur ochrony danych osobowych przez pracowników upoważnionych do przetwarzania danych osobowych jest traktowane jako ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy.
2. Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej.

§ 14
POSTĘPOWANIE W PRZYPADKU STWIERDZENIA NARUSZENIA BEZPIECZEŃSTWA INFORMACJI

1) Każdy pracownik zobowiązany jest zawiadomić ADO i IOD o naruszeniu lub podejrzeniu naruszenia bezpieczeństwa informacji, a w szczególności o:
   a) informacji o wykryciu wirusa w komputerze;
   b) braku dostępu do danych w komputerze;
   c) zablokowaniu czy zepsuciu się komputera czy innego sprzętu;
   d) pozostawieniu dokumentów bez opieki;
   e) przekazaniu maila czy dokumentów z danymi osobie nieupoważnionej;
   f) zgubieniu/zniszczeniu oryginałów dokumentów zawierających dane osobowe;
   g) zgubieniu/zniszczeniu płyty CD/pendrive z dokumentami;
   h) wykasowaniu danych z komputera;
   i) wycieku danych;
   j) pozostawieniu osoby nieupoważnionej bez nadzoru w pomieszczeniu, gdzie są dokumenty, dane;
   k) niewyłączaniu komputera, gdy jest to niepotrzebne;
   l) ustawieniu monitora w ten sposób, że osoby nieupoważnione widzą co mam na pulpicie;

m) kradzieży komputera, dokumentów.

2) Do czasu poinformowania ADO i IOD, należy:
   a) o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn i sprawców;
   b) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę;
   c) przygotować dokładny opis zdarzenia jakie miało miejsce;
3) **Zgłaszanie naruszeń i incydentów związanych z ochroną danych osobowych należy realizować następująco:**
   a) **pracownik placówki / nauczyciel niezwłocznie informuje o zdarzeniu Dyrektora placówki;**
   b) **Dyrektor placówki niezwłocznie powiadamia Inspektora Ochrony Danych o zaistniałym incydencie / naruszeniu;**
   c) **Inspektor Ochrony Danych pomaga Dyrektorowi placówki w uzupełnieniu formularza dla organu nadzorczego, któremu dokument ten przesyłany jest niezwłocznie dostępnymi kanałami (przesłanie następuje nie później niż 72 godziny od zdarzenia).**
4) 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**.
5) 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**.
6) Ostateczną decyzję o zakwalifikowaniu zdarzenia do kategorii naruszeń i zgłoszeniu do PUODO podejmuje Dyrektor, po uprzedniej konsultacji z Inspektorem Ochrony Danych;

§ 15
POSTANOWIENIA KOŃCOWE

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dostępem do przetwarzania danych osobowych z zapisami niniejszego dokumentu w zakresie ochrony danych osobowych.

Dyrektor Szkoły
mgr Iwona Zwinkowska

ZESTAWIENIE ZAŁĄCZNIKÓW DO POLITYKI BEZPIECZEŃSTWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

ZAŁACZNIK NR 1:

WZÓR UPOWAŻIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH WRAZ Z OŚWIADCZENIEM O ZACHOWANIU POUFNOŚCI

ZAŁACZNIK NR 2:

WZÓR UMOWY POWIERZENIA DANYCH OSOBOWYCH

ZAŁACZNIK NR 3:

WZÓR FORMULARZA ZGÓD DLA UCZNIÓW / WYCHOWANYKÓW I ICH RODZICÓW / PRAWNYCH OPIEKUNÓW

ZAŁACZNIK N R 4:

WZÓR REJESTRU UZYSKANYCH ZGÓD

ZAŁACZNIK NR 5:

WZÓR REJESTRU UMÓW POWIERZENIA ZAWARTYCH PRZEZ PUBLICZNĄ PLACÓWKĘ OŚWIATOWĄ

ZAŁACZNIK NR 6:

WZÓR REJESTRU NARUSZEŃ I INCYDENTÓW W ZAKRESIE OCHRONY DANYCH OSOBOWYCH.

ZAŁACZNIK NR 7

WZÓR REJESTRU UPOWAŻNIONYCH PRACWONIKÓW.

ZAŁACZNIK NR 8

WZÓR OŚWIADCZENIA PRACOWNIKA O ZAPOZNANIU SIĘ Z ZASADAMI PRZETWARZANIA DANYCH OSOBOWYCH W ZWIĄZKU Z PRZETWARZANIEM DANYCH NA PRYWATNYCH URZĄDZENIACH INFORMATYCZNYCH / NOŚNIKACH DANYCH

Bydgoszcz, dn. .....

Dyrektor Szkoły/Sekretarz Szkoły

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr .....

Na podstawie art.29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) upoważniam:

.....

do przetwarzania danych osobowych w ramach wykonywania poniższych czynności:

- .....

- .....

Upoważnienie jest ważne od ..... do odwołania. Upoważnienie traci swą ważność w przypadku rozwiązywania lub ustania stosunku pracy .

.....

podpis Dyrektora

Rozdzielnik:

- akta osobowe

....
(imię i nazwisko)

Bydgoszcz dnia .....

.....
(stanowisko)

OŚWIADCZENIE O ZACHOWANIU TAJEMNICY DANYCH OSOBOWYCH

Oświadczam, że zobowiązuję się do:

1. zachowania w tajemnicy, również po ustaniu stosunku pracy:
    - danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych;
    - Informacji o wdrożonych zabezpieczeniach technicznych, organizacyjnych i informatycznych dotyczących danych osobowych;
2. wykorzystywania danych osobowych wyłącznie w celach związanych z wykonywaniem zadań służbowych lub obowiązków pracowniczych;
3. przestrzegania zasad zawartych w „Kodeksie postępowania w zakresie ochrony danych osobowych w publicznych placówkach oświatowych, dla których organem prowadzących jest Miasto Bydgoszcz".

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy.

.....
podpis pracownika

Umowa powierzenia przetwarzania danych osobowych nr .....

zawarta w dniu ..... r. w Bydgoszczy, pomiędzy:

..... **„Powierzającym"**, reprezentowanym przez:
1) ..... – Dyrektora **(wpisać odpowiednio dla pubicznej placówki oświatowej)**

a
..... ,
zwaną w dalszej części umowy **„Przetwarzającym"**, reprezentowaną przez:
1) .....
2) .....

zwani każdy z osobna Stroną, a łącznie Stronami.

Preambuła

Niniejsza umowa zostaje zawarta w związku z umową nr ..... z dnia ..... r., zawartą pomiędzy ..... a ..... w celu .....

§1 Definicje

W Umowie poniższe słowa i wyrażenia oznaczają, co następuje:

1) **Umowa** – oznacza niniejszą umowę powierzenia przetwarzania danych osobowych zawartą przez Strony;
2) **Umowa Główna** – umowa nr ..... zawarta w dniu .....pomiędzy .....;
3) **Rozporządzenie** - ROZPORZĄDZENIE 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).

§2 Postanowienia

1. Powierzający jako administrator danych osobowych w rozumieinu art. 4 pkt 7 Rozporządzenia, działając w trybie art. 28 i 29 Rozporządzenia, powierza Przetwarzającemu jako podmiotowi przetwarzającemu w rozumieniu art. 4 pkt 8 Rozporządzenia, przetwarzanie danych osobowych wyłącznie w celu i na zasadach określonych w Umowie.

§3 Zakres, cel i charakter powierzenia

1. Przedmiotem niniejszej umowy jest powierzenie przetwarzania danych osobowych
   NA PRZYKŁAD: *dane uczniów szkoły*
   w zakresie zakresie: NA PRZYKŁAD: *Imię, Nazwisko, PESEL, imiona rodziców, ...*

2. Przetwarzający zobowiązuje się do przetwarzania danych osobowych, o których mowa w ust. 1, wyłącznie w celu i zakresie niezbędnym dla realizacji zapisów Umowy Głównej. Powierzenie danych osobowych ma na celu umożliwienie Przetwarzającemu realizację poniższych czynności:
   <należy wymienić, opisać czynności powierzone Przetwarzającemu> np.:
   a. *obsługę placówki oświatowej w ramach:*
      i. *wystawienia faktur za obsługę informatyczną placówki oświatowej,*
      ii. *konserwacja sprzętu , na którym znajdują się programy zawierające dane osobowe*
      iii. *dostarczenia placówce oświatowej systemu ewidencyjnego postępów w nauczaniu uczniów*
3. Dane o których mowa w ust. 1 będą przekazywane pomiędzy stronami w formie np. forma papierowa, zewnętrzne nośniki danych, dostęp do systemu informatycznego itd., w okresach np. jednorazowe przekazanie danych, cykliczna wymiana danych, stały dostęp do danych itd.
4. W celu zapewnienia bezpieczeństwa przekazywania danych Strony zastosują następujące zabezpieczenia: np. dokumenty przesyłane za potwierdzeniem odbioru, szyfrowanie nośników danych, dostęp do systemów informatycznych za pomocą szyfrowanego łącza (VPN,https itp.) itd.

§4 Czas obowiązywania umowy

1. Niniejsza umowa zostaje zawarta na czas określony i równy czasowi trwania Umowy Głównej.

§5 Oświadczenie przetwarzającego

1. Przetwarzający oświadcza, że w związku z realizacją umowy, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zapewnia wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, tak by przetwarzanie spełniało wymogi Rozporządzenia i chroniło prawa osób, których dane dotyczą.
2. Przetwarzający oświadcza, że do przetwarzania powierzonych na mocy Umowy danych będą dopuszczone wyłącznie osoby, które złożyły oświadczenie o zachowaniu ich w tajemnicy oraz posiadające upoważnienia do przetwarzania danych osobowych nadane przez Przetwarzającego.
3. Przetwarzający ponosi pełną odpowiedzialność za działania i zaniechania osób upoważnionych przez niego do przetwarzania danych osobowych.
4. Przetwarzający oświadcza, że nie przekazuje danych odsbowych do państw trzecich lub organizacji międzynarodowych czyli poza Europejski Obszar Gospodarczy (EOG). Przetwarzający oświadcza również, że korzysta z podwykonawców przekazujących dane osobowe poza obszar EOG.

§6 Obowiązki i uprawnienia przetwarzającego

1. Przetwarzający zobowiązany jest, przed przystąpieniem do przetwarzania danych osobowych i nie później niż 14 dni od daty zawarcia niniejszej Umowy, do przekazania Powierzającemu ....
   Należy uzupełnić wskazując właściwy dokument np. kopia obowiązującej u Przetwarzającego dokumentacji bezpieczeństwa danych osobowych, w zakresie dotyczącym realizacji czynności, o których mowa w §3 ust.2 lub inny dokument np. certyfikat gwarantujący, że podmiot przetwarzających wdrożył odpowiednie środki techniczne i organizacyjne, by przetwarzanie spełniało wymogi Rozporządzenia i chroniło prawa osób, których dane dotyczą.
2. Przetwarzający uprawniony jest do udzielania upoważnień do przetwarzania danych osobowych powierzonych na mocy niniejszej Umowy.
3. Przetwarzający zobowiązany jest do prowadzenia ewidencji osób, którym nadał upoważnienie do przetwarzania danych osobowych przetwarzanych na podstawie Umowy. Ewidencja musi zawierać informacje zarówno o upoważnieniach aktualnych jak i tych które utraciły moc.
4. Przetwarzający zobowiązany jest do zapewnienia wglądu do ewidencji o której mowa w ust. 3 wskazanym pracownikom Powierzającego.
5. Przetwarzający zobowiązuje się do wykonania wszelkich niezbędnych działań, aby osoby, które zostaną upoważnione do przetwarzania danych osobowych zachowały w tajemnicy dane osobowe także po wygaśnięciu zawartych z nimi umów o pracę oraz innych tytułów kształtujących stosunek pracy lub wszelkich innych umów, porozumień i tytułów, na podstawie których osoby te świadczyły usługi na rzecz Przetwarzającego.
6. Przetwarzający zobowiązany jest do poddania się kontroli w zakresie stosowania przez niego zapisów Rozporządzenia oraz obowiązków wynikających z Umowy.
7. Kontrola, o której mowa w ust. 6 może zostać przeprowadzona przez Powierzającego i obejmować: wgląd do dokumentacji dotyczącej bezpieczeństwa przetwarzania danych osobowych w zakresie wynikającym z Umowy, weryfikację stosowanych przez Przetwarzającego zabezpieczeń również w miejscach przetwarzania danych.
8. Kontroli, o której mowa w ust. 7, Powierzający może dokonać po uprzednim zawiadomieniu przetwarzającego na co najmniej 7 dni roboczych przed planowaną kontrolą.
9. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Powierzającego o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Przetwarzającego danych osobowych określonych w Umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach.
10. Przetwarzający zobowiązuje się do niezwłocznego, nie później niż w ciągu 24 godzin, zgłoszenia Powierzającemu wszelkich stwierdzonych naruszeń ochrony danych osobowych.
11. Przetwarzający zobowiązuje się do przekazania Powierzającemu wszelkich informacji niezbędnych dla przeprowadzenia oceny skutków przetwarzania oraz analizy ryzyka.
12. Przetwarzający zobowiązuje się do wykonywania poleceń administratora w celu wywiązania się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO.

§7 Zachowanie poufności

1. Strony zobowiązują się do zachowania w tajemnicy informacje lub materiały dotyczące każdej ze stron lub działalności przez nią prowadzonej w szczególności dotyczące

zabezpieczeń technicznych i organizacyjnych stosownych w związku z wykonywaniem Umowy.

§8 Dalsze powierzanie

1. Powierzający wyraża ogólną zgodę na to, by Przetwarzający korzystał z usług innego podmiotu przetwarzającego (Podwykonawcy), przy czym:
   a. Podwykonawca winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Przetwarzającego w niniejszej Umowie.
   b. Przetwarzający odpowiada za działania Podwykonawcy, któremu powierzył przetwarzanie danych jak za własne.
   c. Przetwarzający jest zobowiązany do poinformowania Powierzającego o zamiarze dalszego powierzenia przetwarzania nie później niż 14 dni roboczych przed planowaną datą jego rozpoczęcia.
   d. Powierzający ma prawo wniesienia sprzeciwu wobec dalszego powierzania danych w ciągu 14 dni roboczych od daty potwierdzonego doręczenia informacji o której mowa w ust 1 lit c.
2. Powierzający wyraża zgodnę by Przetwarzający korzystał z usług innych podmiotów przetwarzających wymienionych w załączniku nr 1 dołączanym do niniejszej umowy (PUNKT FAKULTATYWNY – niezbędny w przypadku kiedy lista podmiotów jest znana w momencie zawierania umowy powierzenia danych)

§9 Rozwiązanie umowy

1. Powierzający może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Przetwarzający:
   a. pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b. przetwarza dane osobowe w sposób niezgodny z Umową;
   c. powierzył przetwarzanie danych osobowych innemu podmiotowi pomimo sprzeciwu Powierzającego.
2. W przypadku rozwiązania Umowy Przetwarzający jest bezwzględnie zobowiązany do zwrotu powierzonych mu danych osobowych oraz ich kopii lub ich skutecznego usunięcia w celu wyeliminowania możliwości dalszego przetwarzania danych osobowych powierzonych na podstawie niniejszej Umowy.
3. Zwrotowi podlega wszelka dokumentacja związana z przekazanymi danymi osobowymi, w terminie 14 dni od daty rozwiązania Umowy.
4. W terminie 14 dni od daty rozwiązania Umowy Przetwarzający przekaże Powierzającemu protokoły zniszczenia kopii i usunięcia danych osobowych.

§10 Odpowiedzialność

1. Przetwarzający odpowiada za ewentualne szkody, jakie powstaną wobec Powierzającego w związku z niezgodnym z Umową przetwarzaniem przez Przetwarzającego powierzonych danych osobowych. W zakresie w jakim jest to dopuszczalne w świetle obowiązujących przepisów prawa łączna i całkowita odpowiedzialność odszkodowawcza Przetwarzającego wobec Powierzającego, nie może przekroczyć wysokości strat faktycznie poniesionych.
2. W przypadku naruszenia zasad ochrony danych osobowych z przyczyn leżących po stronie Przetwarzającego lub osób działających w jego imieniu, w następstwie którego:
   a. powierzający zostanie zobowiązany prawomocnym wyrokiem sądu lub organu

administracji do wypłaty odszkodowania lub ukarany grzywną, Przetwarzający zobowiązuje się zrekompensować Powierzającemu poniesione z tego tytułu szkody oraz koszty postępowania, włączając kary nałożone na pracowników Powierzającego;

b. z uwagi na wysokie ryzyko naruszenia praw lub wolności osób fizycznych powstanie obowiązek zawiadomienia osób, których dane dotyczą o zaistniałym naruszeniu Przetwarzający zobowiązuje się zrekompensować Powierzającemu poniesione z tego tytułu koszty.

§11 Współpraca Stron

1. Strony ustalają, że podczas realizacji Umowy będą ze sobą ściśle współpracować, informując się wzajemnie o wszystkich okolicznościach mających lub mogących mieć wpływ na wykonanie Umowy, w szczególności obowiązek współpracy dotyczy wzajemnego przekazywania informacji oraz dokonywania ustaleń w zakresie bezpieczeństwa danych osobowych przez osoby pełniące funkcje Inspektorów Ochrony Danych.

§12 Postanowienia końcowe

1. W sprawach nieuregulowanych Umową, zastosowanie znajdują odpowiednie przepisy prawa, w tym w szczególności przepisy Rozporządzenia oraz przepisy Kodeksu Cywilnego.
2. Wszelkie zmiany do umowy muszą być sporządzone w formie pisemnej pod rygorem nieważności.
3. Wszelkie spory wynikające z wykonywania Umowy Strony będą starały się rozstrzygać polubownie, a w przypadku braku możliwości dojścia do porozumienia, rozstrzygać je będzie sąd powszechny właściwy dla siedziby Powierzającego.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze Stron.

Powierzający **Przetwarzający**

Klauzula informacyjna

1. Administratorem Państwa danych osobowych jest Szkota Podstawowa nr 58 im. Ireny Sendlerowej ul. Gdańska 53A, 85-005 Bydgoszcz
2. W sprawach związanych z ochroną swoich danych osobowych możecie się Państwo kontaktować z inspektorem Ochrony Danych za pomocą e-mail: **iod@um.bydgoszcz.pl**
3. Dane osobowe są przetwarzane na podstawie wyrażonej zgody.
4. Dane osobowe będą przetwarzane w celu prezentowania wykonanych prac plastycznych, osiągnięć dziecka jak również informowania o istotnych wydarzeniach życia placówki oraz jej promocji.
5. Niewyrażenie zgody będzie skutkowało brakiem możliwości umieszczenia informacji o osiągnięciach Państwa dziecka w ramach prowadzonych konkurs6w i innych działań promocyjnych.
6. Dane będą udostępniane wyłącznie w ramach konkursów.
7. Do danych osobowych mogą mieć dostęp pracownicy administratora danych na podstawie wydanych upoważnień, a takie m.in. osoby znajdujące się w komisjach konkursowych, osoby korzystające ze strony internetowej, w tym portali społecznościowych w/w podmiotu.
8. Dane osobowe przetwarzane będą do momentu cofnięcia przez Państwa zgody.
9. Dane osobowe mogą być przekazane do organizacji międzynarodowych, które współrealizują projekty edukacyjne, a takie firmy wspomagające w/w podmiot przy organizowaniu imprez okolicznościowych na podstawie zawartych um6w powierzenia przetwarzania danych osobowych.
10. W związku z przetwarzaniem danych osobowych jesteście Państwo uprawnieni do:
    a. Dostępu do danych osobowych.
    b. Poprawiania danych osobowych.
    c. Cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
    0 wycofaniu zgody należy powiadomię w formie pisemnej i mailowej Administratora Danych Osobowych.
    d. Wniesienia żądania usunięcia danych w przypadku cofnięcia zgody na ich przetwarzanie.
    e. Wniesienia żądania ograniczenia przetwarzania danych wyłącznie do ich przechowywania w przypadku:
        i. zakwestionowania prawidłowości danych lub podstawy prawnej ich przetwarzania,
        ii. potrzeby zapobieżenia usunię c ia Państwa danych, pomimo wygarnięcia prawnego tytułu do ich przetwarzania przez Szkot w celu umożliwienia Państwu ustalenia, dochodzenia lub obrony roszczeń,
        iii. do otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych, które zostały dostarczone administratorowi, oraz przestania ich innemu administratorowi (wyłącznie w przypadku przetwarzania danych z użyciem system6w informatycznych).
        iv. Wniesienia skargi do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych.
11. Dane osobowe nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
12. Dane mogą być przekazywane do państwa trzeciego znajdujące się poza obszarem Unii Europejskiej.

.....
imię i nazwisko ucznia wychowanka

Bydgoszcz, dnia .....

.....
klasa grupa

.....
Nazwa placówki (pieczątka placówki oświatowej)

Wyrażam zgodę na upublicznienie danych osobowych w zakresie imię, nazwisko, wiek, grupa, klasa oraz wizerunek dziecka, co do którego sprawuję opiekę prawną, w celu prezentowania wykonanych prac plastycznych, osiągnięć dziecka jak również informowania o istotnych wydarzeniach z życia placówki oraz jej promocji, poprzez:

- stronę internetową placówki

TAK ☐ NIE ☐

- media społecznościowe (np.: facebook.YouTube itp.)

TAK ☐ NIE ☐

- strony internetowe organizacji edukacyjnych współrealizujących z w/w publiczną placówką oświatową projekty edukacyjne w tym organizacji międzynarodowych,

TAK ☐ NIE ☐

- tablice informacyjne (gabloty, tablice multimedialne) w w/w publicznej placówce oświatowej

TAK ☐ NIE ☐

- udział w konkursach

TAK ☐ NIE ☐

- kroniki oraz gazetki szkolne wydane przez w/w publiczną placówkę oświatową

TAK ☐ NIE ☐

Zgoda może zostać wycofana w każdym momencie.

Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

Podpis Rodziców /Prawnych Opiekunów dziecka: .....

Załącznik nr 4 do Kodeksu postępowania
w zakresie ochrony danych osobowych

REJESTR UDZIELONYCH ZGÓD PRZEZ RODZICÓW W ZWIĄZKU Z UCZĘSZCZANIEM DZIECKA DO .....

L.p.	*Imię i nazwisko dziecka*	*Zgoda*							*Data udzielonej zgody*	*Data cofnięcia zgody*
		Prezentowanie prac plastycznych	*Uczestnictwo w konkursach*	*Zdjęcia i filmy z imprez okolicznościowych i plenerowych*	*Zdjęć i filmy z zajęć dydaktyczno - wychowawczych*	*Na udział w zajęciach poza siedzibą .....*	*Udział w wycieczce*	....		
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										
20										
21										
22										

Rejestr umów powierzenia danych osobowych

L.p.	Nr umowy	Data zawarcia umowy	Strona umowy	Kategorie osób, których dane dotyczą	Zakres powierzonych danych	Zakres czynności przetwarzania
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						

Rejestr naruszeń ochrony danych osobowych

L.p.	Rodzaj naruszenia / incydentu	Data stwierdzenia naruszenia/ incydentu	Obowiązek zgłoszenia organowi nadzorczemu – PUODO	Obowiązek zawiadomienia osoby, której dane dotyczą TAK / NIE	Okoliczności naruszenia/ incydentu	Skutki naruszenia/ incydentu	Podjęte działania zaradcze	Data powiadomienia Inspektora Danych Osobowych (IOD)
1								
2								
3								
4								
5								

Rejestr osób upoważnionych
do przetwarzania danych osobowych

lp.	Imię i nazwisko osoby upoważnionej	Zajmowane stanowisko	Nr upoważnienia	Data		Podpis wydającego upoważnienie
				nadania upoważnienia	wygaśnięcia upoważnienia	
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Bydgoszcz, dn. .....

.....
Imię i nazwisko pracownika

OŚWIADCZENIA PRACOWNIKA O ZAPOZNANIU SIĘ Z ZASADAMI PRZETWARZANIA DANYCH OSOBOWYCH NA PRYWATNYCH URZĄDZENIACH INFORMATYCZNYCH / NOŚNIKACH DANYCH

Zobowiązuję się do stosowania zasad przetwarzania danych osobowych na urządzeniach informatycznych prywatnych i nośnikach danych , w tym ograniczeniu dostępu do danych osobowych członkom rodziny i osobom postronnym zgodnie z w *§ 11 Bezpieczeństwo informatyczne Kodeksu postępowania w zakresie ochrony danych osobowych w publicznych placówkach oświatowych,*
dla których organem prowadzącym jest Miasto Bydgoszcz.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższym zobowiązaniem, może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy.

.....
podpis pracownika