POLITYKA OCHRONY DANYCH
W ZESPOLE SZKÓŁ OGÓLNOKSZTAŁCĄCYCH NR 3 W SZCZECINIE

Spis treści

Wersja dokumentacji:	1
Data:	25.05.2018 r.
Polityka przygotowana przez:	Zespół RODO powołany w ZSO 3
Zatwierdzone przez zarząd / kierownictwo:	Dyrektora ZSO 3
Polityka zaczęła działać od:	25.05.2018 r.
Data następnego przeglądu:	24.05.2019 r.
Ostatnia aktualizacja:	25.05.2018 r.
Administrator Danych:	Zespół Szkół Ogólnokształcących Nr 3
Inspektor Ochrony Danych:	Joanna Litwin

1. Podstawowe definicje

1.1. **ADO (Administrator danych) –** Zespół Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin) samodzielnie lub z innymi ADO ustala cele i sposoby przetwarzania danych osobowych.

1.2. **Podmiot przetwarzający -** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu ADO;

1.3. **Inspektor ochrony danych (IOD) -** osoba wyznaczona przez ADO posiadająca kwalifikacje zawodowe, a w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych oraz posiadająca umiejętności wypełnienia zadań polegających m.in. na nadzorowaniu przestrzegania zasad ochrony danych osobowych. IOD bezpośrednio podlega najwyższemu kierownictwu ADO, może być członkiem personelu ADO lub wykonywać zadania na podstawie umowy o świadczenie usług.

1.4. **Dane osobowe -** 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.

1.5. **Szczególne kategorie danych (tzw. dane wrażliwe) -** dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

1.6. **Personel -** osoby zatrudnione na podstawie stosunku pracy, umów cywilnoprawnych (umowa o dzieło, umowa zlecenia), osoby odbywające praktyki, stażyści, osoby skierowane do pracy w ramach umów z agencjami pracy tymczasowej, osoby samozatrudnione, wykonujące prace związane z przetwarzaniem danych osobowych u ADO (Osoby te pracują na sprzęcie należącym do ADO oraz nie są zaangażowane w projekty z innymi podmiotami). W szczególności przez personel ADO rozumie się pracowników dydaktycznych, administracyjnych i techniczno-fizycznych.

1.7. **Odbiorca danych -** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Nie uznaje się za odbiorców organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem krajowym - przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

1.8. **Rejestr systemów**[1] **-** rejestr wszystkich systemów, w których dane osobowe są przetwarzane przez ADO.

[1] Rejestr ten stanowi załącznik nr 3 do niniejszej polityki

1.9. **Kontrahent- dostawca –** oznacza osobę fizyczną lub prawną, będącą podmiotem świadczącym usługi lub dostarczającym dobra dla ADO (np. firma ochroniarska, firma sprzątająca, podwykonawca).

1.10. **Profilowanie** - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

1.11. **Wykaz skrótów:**

1.11.1. **ADO -** Administrator danych osobowych: Zespół Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin),

1.11.2. **Polityka** – niniejszy dokument, stanowiący Politykę Ochrony Danych,

1.11.3. **IOD –** Inspektor Ochrony Danych,

1.11.4. **RODO -** 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),

1.11.5. **UODO -** Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz.1000),

1.11.6. **PUODO –** Prezes Urzędu Ochrony Danych Osobowych.

2. Wprowadzenie

2.1. ADO gromadzi i wykorzystuje określone informacje o osobach. Tymi osobami mogą być uczniowie, rodzice/opiekunowie prawni uczniów, Personel, Kontrahenci i inne osoby, z którymi ADO ma kontakt lub w przyszłości taki kontakt może okazać się potrzebny.

2.2. Niniejsza polityka opisuje sposób gromadzenia, przetwarzania i przechowywania tych danych osobowych w celu spełnienia standardów ochrony danych podmiotu oraz przestrzegania przepisów prawa.

2.3. Polityka ochrony danych zapewnia przez ADO:

2.3.1. Przestrzeganie przepisów o ochronie danych i przestrzeganie dobrych praktyk,

2.3.2. Ochronę praw Personelu, uczniów, rodziców/opiekunów prawnych uczniów, Kontrahentów oraz innych osób, których dane ADO przetwarza.

2.3.3. Informację na temat tego, jak przechowuje i przetwarza się dane osób,

2.3.4. Ochronę przed naruszeniem danych.

2.4. Podstawy prawne przygotowania polityki stanowią:

2.4.1. 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),

2.4.2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018, poz.1000).

2.5. Obowiązki określone w niniejszej polityce mają zastosowanie odpowiednio do wszystkich:

2.5.1. danych osobowych przetwarzanych przez Zespół Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin), zarówno w przypadku, gdy jest ADO, jak i w sytuacji, gdy jest podmiotem przetwarzającym,

2.5.2. nośników informacji, np. papierowych, magnetycznych, optycznych itp., na których są lub będą znajdować się dane osobowe,

2.5.3. lokalizacji - budynków i pomieszczeń ADO, w których są lub będą przetwarzane dane osobowe,

2.5.4. osób stanowiących Personel,

2.5.5. innych osób mających dostęp do danych osobowych.

2.6. Osoby stanowiące Personel ADO oraz wszystkie inne mające dostęp do tych danych zobowiązane są do przestrzegania postanowień Polityki.

2.7. Polityka nie obejmuje obszaru i systemu informatycznego oraz środków technicznych i organizacyjnych zastosowanych przez podmioty, którym zostały powierzone dane osobowe w drodze umowy zawartej na piśmie.

2.8. W zakresie nieuregulowanym w niniejszej Polityce do przetwarzania danych osobowych zastosowanie mają przepisy RODO, UODO oraz przepisów odrębnych regulujących przetwarzanie danych osobowych u ADO.

3. Obowiązki w zakresie danych osobowych

3.1. Każdy, kto pracuje u ADO ponosi odpowiedzialność za zapewnienie, że dane są odpowiednio zbierane, przechowywane i obsługiwane.

3.2. Obowiązki ADO obejmują:

3.2.1. Zapewnienie środków technicznych i organizacyjnych do ochrony przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną, w szczególności zabezpieczenie danych przed:

- udostępnieniem osobom nieupoważnionym,
- zabraniem przez osobę nieuprawnioną,
- zmianą, utratą, uszkodzeniem lub zniszczeniem.

3.2.2. Środki techniczne i organizacyjne, o których mowa w 4.2.1. to w szczególności:

- pseudonimizacja i szyfrowanie danych osobowych,

• zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

• zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,

• regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych, które mają zapewnić bezpieczeństwo przetwarzania.

3.2.3. Zapewnienie legalności przetwarzania danych osobowych, a w szczególności zadbanie, by:

- została pozyskana zgoda osoby, której dane dotyczą lub została spełniona inna przesłanka dopuszczająca przetwarzanie danych osobowych,
- został spełniony obowiązek informacyjny wobec osoby, której dane dotyczą,
- dane były przetwarzane zgodnie z obowiązującymi przepisami prawa, dobrymi praktykami oraz normami społecznymi,
- dane zbierane były w oznaczonym zgodnym z prawem celu,
- dane były merytorycznie poprawne oraz zakres danych był adekwatny do celu zbierania,
- dane były przetwarzane z ograniczeniem czasowym.

3.2.4. Zatwierdzenie dokumentacji opisującej sposób przetwarzania danych osobowych, w szczególności:

- Polityki przetwarzania danych osobowych,
- Rejestru czynności przetwarzania danych osobowych
- Rejestru kategorii czynności przetwarzania danych osobowych,
- Oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych przez ADO.

3.2.5. Określenie kategorii danych oraz operacji wykonywanych na danych, które są niezbędne do realizacji zadań i obowiązków na danym stanowisku. Obowiązek ten może zostać delegowany na bezpośrednich przełożonych osób upoważnianych.

3.2.6. Dopuszczanie do przetwarzania danych wyłącznie osób przeszkolonych i upoważnionych do przetwarzania danych, a także wydawanie poleceń do przetwarzania danych. Wzór ewidencji osób upoważnionych do przetwarzania danych stanowi załącznik nr 4 do Polityki.

3.2.7. Nadzorowanie i dbanie o zgodne z prawem przekazywanie danych osobowych (udostępnianie i powierzanie). Wzór umowy powierzenia stanowi załącznik nr 14 do Polityki.

3.2.8. Respektowanie praw osób, których dane dotyczą, a w szczególności prawa do uzyskania informacji o:

- ADO i IOD,
- celu i podstawie prawnej przetwarzania danych,
- profilowaniu i skutkach profilowania,
- prawnie uzasadnionych interesach realizowanych przez ADO lub przez stronę trzecią,
- odbiorcach danych lub ich kategoriach,
- o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
- okresie, przez który dane osobowe będą przechowywane,
- prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania, a także o prawie do przenoszenia danych, cofnięcia zgody,
- informacje o prawie wniesienia skargi do organu nadzorczego;
- czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
- jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle.

3.2.9. Respektowanie praw osób, których dane dotyczą w zakresie:

- prawa dostępu do danych i informacji o nich: art. 13-15 RODO ,
- prawa do sprostowania danych: art. 16 RODO,
- prawa do usunięcia danych- ,,prawo do bycia zapomnianym'': art. 17 RODO,
- prawa do ograniczenia przetwarzania: art. 18 RODO,
- prawa do przeniesienia danych: art. 20 RODO,
- prawa do sprzeciwu: art. 21 RODO,
- prawa do wycofania zgody na przetwarzanie danych osobowych: art. 7 ust. 3 RODO.

3.2.10. Zapewnienie przeprowadzania regularnych wewnętrznych sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Częstotliwość przeprowadzania sprawdzeń jest określana przez IOD zarządzeniem.

3.2.11. Powołanie IOD nadzorującego przestrzeganie zasad ochrony w przypadku, w którym ADO nie wykonuje tych obowiązków sam.

3.3. Obowiązki osoby pełniącej funkcję Inspektora Ochrony Danych (IOD) obejmują:

3.3.1. Monitorowanie przestrzegania RODO, innych przepisów Unii Europejskiej oraz prawa polskiego o ochronie danych oraz niniejszej Polityki w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia Personelu, oraz powiązane z tym audyty.

3.3.2. Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania.

3.3.3. Współpraca z organem nadzorczym, czyli Prezesem Urzędu Ochrony Danych Osobowych (PUODO).

3.3.4. Pełnienie funkcji punktu kontaktowego dla PUODO w kwestiach związanych z przetwarzaniem oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

3.3.5. Przygotowanie planu sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

3.3.6. Dokonywanie planowych sprawdzeń zgodności przetwarzania danych osobowych z przepisami oraz dokumentacją ochrony danych osobowych.

3.3.7. Przygotowanie sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych dla ADO.

3.3.8. Przygotowywanie zawiadomień dla ADO w przypadku nieopracowania, braków lub nieaktualności dokumentacji ochrony danych osobowych.

3.3.9. Przygotowywanie pouczeń lub instrukcji dla osób nieprzestrzegających zasad określonych w dokumentacji przetwarzania danych osobowych o prawidłowym sposobie ich realizacji lub zawiadamianie ADO o osobach odpowiedzialnych za naruszenie przepisów.

3.3.10. Nadzorowanie opracowania i aktualizowania dokumentacji ochrony danych osobowych ADO.

3.3.11. Zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

3.3.12. Wzór powołania Inspektora Ochrony Danych stanowi załącznik nr 4 do Polityki.

3.4. Obowiązki Personelu obejmują:

3.4.1. Zapoznanie się i stosowanie obowiązujących przepisów prawa w zakresie ochrony danych osobowych.

3.4.2. Zapewnienie bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem.

3.4.3. Informowanie przełożonych o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu ochrony danych osobowych.

3.4.4. Przestrzeganie tzw. „zasady czystego biurka” - na biurku powinny znajdować się jedynie dokumenty potrzebne do wykonania bieżącej pracy.

3.4.5. Niszczenie zbędnych dokumentów papierowych oraz nośników zawierających dane osobowe w niszczarkach lub umieszczanie ich w specjalnie do tego celu przygotowanych pojemnikach.

3.4.6. Dbanie o to, by dokumenty zawierające dane osobowe były przechowywane w zamkniętych szafach lub szufladach, lub w inny sposób uniemożliwiający dostęp osobom nieupoważnionym.

3.4.7. Dbanie, aby osoby postronne (np. goście) poruszały się po pomieszczeniach, w których przetwarzane są dane osobowe tylko przy asyście osób zatrudnionych.

3.4.8. W odniesieniu do sprzętu komputerowego i urządzeń teleinformatycznych, a także w związku z korzystaniem z zasobów systemów i aplikacji służących do przetwarzania danych każda osoba jest zobowiązana do dbania o bezpieczeństwo użytkowanego komputera, w tym celu użytkownik ma obowiązek:

- informować przełożonych w przypadku wykrycia zagrożenia lub o fakcie posiadania praw dostępu do zasobów, do których nie powinien mieć dostępu,
- blokować dostęp do komputera podczas opuszczania stanowiska pracy (np. włączać wygaszacz ekranu chroniony hasłem lub wylogowywać się z systemu),
- niezwłocznie zmienić hasło, jeśli istnieje podejrzenie, że hasło mogło zostać poznane przez inna osobę,
- stosować następujące zasady w stosunku do haseł dostępowych:
  - hasła mogą być zapisywane wyłącznie w postaci zaszyfrowanej,
  - hasła nie mogą być powszechnie używanymi słowami oraz w szczególności nie należy wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów,
  - hasło musi składać się co najmniej z 8 znaków i musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
- wykazywać szczególną ostrożności przy odbieraniu poczty elektronicznej przychodzącej od nieznanych adresatów lub o podejrzanym tytule e-maila,
- dbać, aby komputer wyposażony były w stosowne i na bieżąco aktualizowany program ochrony antywirusowej,
- ekran monitora ustawić tak, aby uniemożliwić wgląd w przetwarzane dane osób nieuprawnionych.

3.4.9. Użytkownicy, którzy korzystają z komputerów, na których przetwarzane są dane osobowe (ma to również zastosowanie do komputerów własnych) powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych. Zaleca się ponadto szczególną ostrożność podczas ich transportu, a w szczególności stosowanie się do poniższych zasad:

- nie wolno pozostawiać komputera przenośnego bez dozoru,
- w samochodzie komputer przenośny należy przewozić albo w zamkniętym bagażniku, albo na podłodze w miejscu przeznaczonym na nogi pasażera,
- zabronione jest odstępowanie komputera przenośnego osobom trzecim,
- przy wychodzeniu z pomieszczenia, w którym zostaje komputer bez nadzoru należy komputer schować do zamykanej szuflady, szafki lub zamknąć pomieszczenie na klucz,
- po zakończonym dniu pracy komputer należy zabezpieczyć przed dostępem osób nieuprawnionych i kradzieżą przez zamknięcie go w szafce lub szufladzie zamykanej na klucz.

3.4.10. Każdy komputer, na którym przetwarzane są dane osobowe musi być dostępny dla ADO.

3.4.11. Nieprzestrzeganie powyższych zasad może skutkować odpowiedzialnością karną zgodnie z UODO oraz wyciągnięciem konsekwencji służbowych zgodnie z kodeksem pracy lub w przypadku umów cywilnych (umowa o dzieło, umowa zlecenia, jednoosobowa działalność gospodarcza) odpowiedzialnością cywilną.

3.4.12. Każda osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do podpisania oświadczenia o zachowaniu poufności. Wzór upoważnienia i oświadczenia stanowi załącznik nr 3 do Polityki.

4. Ogólne wytyczne dla Personelu

4.1. Jedynymi osobami, które mają dostęp do danych objętych tą Polityką, powinny być osoby, które potrzebują ich do swojej pracy.

4.2. Dane nie powinny być udostępniane nieformalnie. Gdy wymagany jest dostęp do poufnych informacji, pracownicy mogą poprosić o nie swoich przełożonych.

4.3. ADO zapewni szkolenia dla wszystkich pracowników, aby pomóc im zrozumieć ich obowiązki związane z przetwarzaniem danych.

4.4. Pracownicy powinni dbać o bezpieczeństwo wszystkich danych, podejmując rozsądne środki ostrożności i postępując zgodnie z poniższymi wytycznymi.

4.5. W szczególności należy używać silnych haseł utworzonych zgodnie z ust. 4.4.8. Polityki i nigdy nie wolno ich udostępniać.

4.6. Dane osobowe nie powinny być ujawniane nieupoważnionym osobom ani w Zespole Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin) , ani na zewnątrz.

4.7. Dane powinny być regularnie przeglądane i aktualizowane, jeśli okaże się, że są nieaktualne. Jeżeli nie są już potrzebne, należy je usunąć.

4.8. Pracownicy powinni zwrócić się o pomoc do swojego przełożonego lub IOD, jeśli nie mają pewności co do jakiegokolwiek aspektu ochrony danych.

4.9. Pracownicy dydaktyczni, w szczególności nauczyciele powinni chronić dane osobowe uczniów przed dostępem osób trzecich i przestrzegać zasad wynikających z niniejszej Polityki zwłaszcza w sytuacji wykonywania pracy w domu na prywatnym komputerze (np. sprawdzanie testów, prac, zeszytów, wpisywanie ocen do elektronicznego dziennika).

4.10. Personel ADO jest obowiązany do zachowania w tajemnicy i nieujawniania osobom nieuprawnionym informacji stanowiących szczególne kategorie danych osobowych, a uzyskanych w związku z pełnioną funkcją lub wykonywaną pracą, dotyczących zdrowia, potrzeb rozwojowych i edukacyjnych, możliwości psychofizycznych, seksualności, orientacji seksualnej, pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub światopoglądowych uczniów.

4.11. Ustępu 5.10. nie stosuje się:

1) w przypadku zagrożenia zdrowia ucznia;

2) jeżeli rodzic/opiekun prawny ucznia, wyrazi zgodę na ujawnienie określonych informacji;

3) w przypadkach gdy przewidują to przepisy szczególne.

4.12. Szczegółowe wytyczne dla Personelu zawarte są w załączniku nr 13 do Polityki.

5. Przetwarzanie danych osobowych w skrzynce e-mail

5.1. W zakresie korzystania z poczty elektronicznej wskazane jest zapewnienie poufności poprzez szyfrowanie przekazywanych informacji lub odpowiednie zabezpieczenie infrastruktury, na którą składają się komputer nadawcy i odbiorcy, serwery pocztowe nadawcy i odbiorcy oraz kanały komunikacyjne do przesyłania informacji między nimi.

5.2. Zaleca się korzystanie z usług dostawców poczty elektronicznej, którzy zapewnią warunki bezpieczeństwa i zachowanie w poufności treści przesyłanej korespondencji.

5.3. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do korzystania z poczty elektronicznej tylko w celach służbowych.

5.4. W przypadku przesyłania danych osobowych poza szkołę należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych, podpis elektroniczny).

5.5. Przy szyfrowaniu można posłużyć się np. programem kompresującym 7-Zip, dostępnym nieodpłatnie w ramach licencji Open Source. Umożliwia on tworzenie samorozkodowujących się plików zawierających zaszyfrowane informacje. Odbiorca takiego pliku, aby zaszyfrowane w nim informacje odczytać, nie musi instalować na swoim komputerze programu 7-Zip. Plik taki zostanie bowiem przez system operacyjny

komputera uruchomiony bez użycia programu 7-Zip. Do odszyfrowania przekazanej w nim informacji niezbędne jest wprowadzenie klucza kryptograficznego (hasła), który został użyty podczas jego tworzenia. Zgodnie z dobrymi praktykami, klucz taki powinien zostać przesłany do odbiorcy innym, bezpiecznym kanałem komunikacji.

5.6. Dodatkową metodą zapewnienia poufności jest użycie serwerów pocztowych, które w komunikacji między komputerem nadawcy i odbiorcy oraz między sobą wykorzystują szyfrowane kanały komunikacyjne. Wysyłający wiadomość musi w takim przypadku posiadać informacje dotyczące zarówno bezpieczeństwa przekazywania informacji między serwerami pocztowymi nadawcy i odbiorcy, jak i między urządzeniami nadawcy i odbiorcy z ich serwerami pocztowymi. Praktycznie rozwiązanie takie może zatem mieć zastosowanie jedynie w przypadku, jeśli nadawca i odbiorca wiadomości wykorzystują do komunikacji między sobą ten sam serwer pocztowy.

5.7. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.

5.8. Każdy użytkownik poczty e-mail przed wysłaniem poczty jest zobowiązany sprawdzić poprawność adresu odbiorcy dokumentu i zweryfikować tożsamość nadawcy Profesjonalnym rozwiązaniem zapewniającym wiarygodną identyfikację adresu e-mail nadawcy oraz skuteczną ochronę przed modyfikacją wiadomości jest stosowanie certyfikatu elektronicznego. Alternatywnym rozwiązaniem może być zakup komercyjnych certyfikatów ID. Należy również wykorzystywać adresy, które w miarę możliwości identyfikują nadawcę już po składni samego adresu, a zatem nie korzystać z prywatnych adresów e-mail w korespondencji służbowej.

5.9. Zaleca się, aby użytkownik podczas przesyłania danych osobowych e-mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

5.10. W celu ochrony przed zainfekowaniem komputera użytkownika i komputerów pracujących w sieci (kryptowirusy) zabrania się otwierania załączników (plików) w mailach nawet od prawdopodobnie znanych użytkownikowi nadawców bez weryfikacji nadawcy.

5.11. Zabrania się, bez weryfikacji wiarygodności nadawcy otwierać hiperlinki zawarte w e-mailach. Nieprzestrzeganie tej zasady może doprowadzić do zainfekowania komputera użytkownika i innych pracujących w sieci.

5.12. Wszystkie przypadki e-maili budzących podejrzenie należy zgłaszać ADO, IOD.

5.13. Przy wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".

5.14. Zabrania się rozsyłania maili z tzw. „ łańcuszkami szczęścia". Adres mailowy służbowy służy wyłącznie do korespondencji służbowej.

5.15. Pracownik ma obowiązek systematycznego czyszczenie poczty z nieaktualnych -e- mali oraz opróżniania kosza.

5.16. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.

5.17. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.

5.18. Korzystanie z poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

5.19. Użytkownicy nie mają prawa korzystać z poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub nietycznym i naruszającym cudzą godność i prywatność

5.20. Zabrania się dokonywanie w sieci zakupów, rezerwacji usług lub świadczeń na rzecz użytkownika oraz dokonywania przelewów bankowych z prywatnego konta.

5.21. Użytkownik bez zgody ADO nie ma prawa wysyłać wiadomości zawierających dane osobowe przetwarzane przez ADO w tym dane Personelu, uczniów, rodziców i opiekunów prawnych oraz Kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

6. Zasady ochrony danych

6.1. ADO zobowiązuje się do przetwarzania danych zgodnie z zasadami wynikającymi z RODO i niniejszej Polityki.

6.2. Zasady te dotyczą wszystkich danych osobowych przetwarzanych przez ADO.

6.3. Osoba odpowiedzialna ponosi odpowiedzialność za ciągłe przestrzeganie zasad, które są określone w niniejszej polityce ochrony danych, przez ADO.

6.4. Zasady te podlegają przeglądowi co najmniej raz w roku.

7. Zgodność z prawem, rzetelność i przejrzystość przetwarzania

7.1. Aby zapewnić, że przetwarzanie danych jest zgodne z prawem, rzetelne i przejrzyste, ADO prowadzi rejestr czynności przetwarzania.

7.2. Nie ma obowiązku, aby prowadzić rejestru czynności przetwarzania w formie papierowej, a z praktycznego punktu widzenia zaleca się jego prowadzenie w formie elektronicznej, np. w programie Microsoft Excel lub Word albo za pomocą specjalnego, dedykowanego do tego celu oprogramowania.

7.3. Rejestr systemów podlega przeglądowi co najmniej raz w roku.

7.4. Osoby fizyczne mają prawo dostępu do swoich danych osobowych, a wszelkie takie prośby skierowane do podmiotu będą rozpatrywane w odpowiednim czasie.

8. Cele zgodne z prawem

8.1. Wszystkie dane przetwarzane przez ADO muszą być wykonywane na jednej z następujących podstaw prawnych: zgoda, umowa, wykonanie obowiązku prawnego, żywotne interesy, zadanie publiczne lub uzasadnione prawne interesy.

8.2. ADO odnotowuje odpowiednią podstawę prawną w rejestrze czynności przetwarzania.

8.3. Jeżeli zgoda jest traktowana jako podstawa przetwarzania danych, dokument potwierdzający wyrażenie zgody powinien być przechowywany razem z danymi osobowymi.

8.4. W przypadku, gdy dochodzi do przetwarzania danych osobowych w oparciu o wyrażoną zgodę, możliwość cofnięcia wyrażonej zgody, przez osobę która ją wyraziła, powinna być łatwo dostępna, a w systemie ADO powinny istnieć mechanizmy zapewniające skuteczność takiego odwołania.

9. Minimalizacja danych

9.1. ADO zapewnia, że dane osobowe są adekwatne, istotne i ograniczone do tego, co jest konieczne w związku z celami, dla których są przetwarzane.

10. Profilowanie

10.1. Profilowanie jako forma przetwarzania danych osobowych wymaga w każdym przypadku wykazania podstawy prawnej dla takiego przetwarzania, o której mowa w art. 6 ust. 1 lub art. 9 ust. 1 RODO. Jeśli profilowanie wiąże się ze zautomatyzowanym, czyli pozbawionym czynnika ludzkiego, podejmowaniem decyzji, która wywołuje skutki prawne względem osoby, której dane są przetwarzane lub w podobny sposób znacząco na nią wpływa, ADO powinien upewnić się, że osoba ta wyraziła na tę decyzję wyraźną zgodę lub decyzja jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a ADO lub decyzja jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega ADO i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

10.2. Osoba, której dane dotyczą, powinna mieć prawo do tego, by nie podlegać decyzji, która ocenia jej czynniki osobowe, opiera się wyłącznie na przetwarzaniu zautomatyzowanym i wywołuje wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób znacząco na nią wpływa. Do takiego przetwarzania zalicza się profilowanie, o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa.

10.3. Zautomatyzowane podejmowanie decyzji to zdolność do podejmowania decyzji środkami technicznymi bez udziału człowieka. Automatyczne podejmowanie decyzji ma inny zakres i może częściowo pokrywać się z profilowaniem.

10.4. Każda osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji w zakresie założeń ewentualnego zautomatyzowanego przetwarzania danych

osobowych oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania.

10.5. Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, powinna mieć prawo wnieść w dowolnym momencie, bezpłatnie sprzeciw wobec tego przetwarzania, pierwotnego lub dalszego - w tym profilowania, o ile jest ono powiązane z marketingiem bezpośrednim.

10.6. Podejmowanie decyzji na podstawie zautomatyzowanego przetwarzania, w tym profilowania, która to decyzja wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa, jest dozwolone, w przypadku gdy jest to wyraźnie dopuszczone prawem Unii lub prawem państwa członkowskiego, któremu podlega ADO, w tym:

10.6.1. do celów monitorowania i zapobiegania oszustwom i uchylaniu się od podatków,

10.6.2. do zapewniania bezpieczeństwa i niezawodności usług świadczonych przez ADO,

10.6.3. gdy jest niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a ADO,

10.6.4. gdy osoba, której dane dotyczą, wyraziła wyraźną zgodę.

10.7. Przetwarzanie takie powinno zawsze podlegać odpowiednim zabezpieczeniom, obejmującym:

10.7.1. informowanie osoby, której dane dotyczą,

10.7.2. prawo do uzyskania interwencji człowieka,

10.7.3. prawo do wyrażenia własnego stanowiska,

10.7.4. prawo do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawo do zakwestionowania takiej decyzji.

10.8. Takie przetwarzanie nie powinno dotyczyć dzieci.

10.9. Aby zapewnić rzetelność i przejrzystość przetwarzania wobec osoby, której dane dotyczą, mając na uwadze konkretne okoliczności i kontekst przetwarzania danych osobowych, ADO powinien stosować:

10.9.1. odpowiednie matematyczne lub statystyczne procedury profilowania,

10.9.2. wdrożyć środki techniczne i organizacyjne zapewniające w szczególności korektę powodujących nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów,

10.9.3. zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą, oraz zapobiegający m.in. skutkom w postaci dyskryminacji osób fizycznych z uwagi na pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan genetyczny lub zdrowotny, orientację seksualną lub skutkujący środkami mającymi taki efekt.

10.10. Zautomatyzowane podejmowanie decyzji i profilowanie oparte na szczególnych kategoriach danych osobowych powinny być dozwolone wyłącznie przy zachowaniu szczególnych warunków.

11. Prawidłowość przetwarzanych danych

11.1. ADO podejmie uzasadnione kroki w celu zapewnienia prawidłowości przetwarzania danych osobowych.

11.2. Tam, gdzie jest to konieczne dla zgodnych z prawem podstaw przetwarzania danych, należy wprowadzić odpowiednie kroki w celu zapewnienia aktualności danych osobowych.

11.3. Prawo wymaga od ADO podjęcia uzasadnionych kroków w celu zapewnienia dokładności i aktualności danych.

11.4. Im ważniejsze jest to, że dane osobowe są prawidłowe, tym większy wysiłek ADO powinien włożyć w zapewnienie ich prawidłowości.

11.5. Obowiązkiem wszystkich członków Personelu, którzy pracują z danymi, jest podjęcie rozsądnych kroków w celu zapewnienia, że przetwarzane dane są poprawne tak jak tylko jest to możliwe.

11.6. Dane będą przechowywane w niewielu miejscach, i tylko gdy istnieje wyraźna potrzeba ich przechowywania.

11.7. Personel nie powinien tworzyć niepotrzebnych dodatkowych zestawów danych.

11.8. Personel powinien wykorzystywać każdą okazję, aby zapewnić aktualizację danych.

11.9. ADO ułatwi osobom, których dane dotyczą, aktualizowanie informacji o nich, jakie posiada, np. za pośrednictwem strony internetowej.

11.10. Dane powinny być aktualizowane, gdy zostaną wykryte niedokładności. Na przykład, jeśli nie można już dotrzeć do rodzica/opiekuna prawnego ucznia na podstawie zapisanego numeru telefon, należy ten numer usunąć z bazy danych.

12. Archiwizacja / usuwanie

12.1. Aby zapewnić, że dane osobowe są przechowywane nie dłużej niż to konieczne, ADO prowadzi politykę archiwizacji dla każdego obszaru, w którym przetwarzane są dane osobowe i corocznie dokonuje przeglądu tego procesu.

12.2. Polityka archiwizacji uwzględnia, jakie dane powinny / muszą zostać zachowane, na jak długo i dlaczego.

13. Bezpieczeństwo i przechowywanie danych

13.1. Zasady te opisują, jak i gdzie dane powinny być bezpiecznie przechowywane. Pytania dotyczące bezpiecznego przechowywania danych można kierować ADO.

13.2. Gdy dane są przechowywane na papierze, powinny być przechowywane w bezpiecznym miejscu, gdzie nieupoważnione osoby nie mogą ich zobaczyć.

13.3. Niniejsze wytyczne mają również zastosowanie do danych, które są zwykle przechowywane elektronicznie, ale które zostały wydrukowane z jakiegoś powodu:

13.3.1. Gdy nie jest to wymagane, kartki lub pliki powinny być przechowywane w zamkniętej szufladzie lub szafce na dokumenty.

13.3.2. Pracownicy powinni upewnić się, że kartki i wydruki nie są pozostawione tam, gdzie mogłyby je zobaczyć osoby nieuprawnione, np. na drukarce.

13.3.3. Wydruki danych powinny zostać zniszczone np. za pomocą niszczarki i usunięte w bezpieczny sposób, gdy nie są już potrzebne.

13.4. Gdy dane są przechowywane elektronicznie, muszą być chronione przed nieautoryzowanym dostępem, przypadkowym usunięciem i złośliwymi próbami włamania:

13.4.1. Dane powinny być chronione silnymi hasłami, które są regularnie zmieniane i nigdy nie są przekazywane między pracownikami.

13.4.2. Jeśli dane są przechowywane na nośnikach wymiennych (takich jak płyty CD lub DVD), powinny być bezpiecznie przechowywane, gdy nie są używane.

13.4.3. Dane powinny być przechowywane wyłącznie na wyznaczonych dyskach i serwerach i powinny być przesyłane wyłącznie do zatwierdzonych usług przetwarzania w chmurze.

13.4.4. Serwery zawierające dane osobowe powinny znajdować się w bezpiecznym miejscu, z dala od ogólnej przestrzeni biurowej.

13.4.5. Dane powinny często być archiwizowane. Kopie zapasowe powinny być regularnie testowane, zgodnie ze standardowymi procedurami tworzenia kopii zapasowych podmiotu.

13.4.6. Dane nigdy nie powinny być zapisywane bezpośrednio na laptopach lub innych urządzeniach mobilnych, takich jak tablety czy smartfony.

13.4.7. Wszystkie serwery i komputery zawierające dane powinny być chronione za pomocą zatwierdzonego oprogramowania zabezpieczającego i zapory.

13.4.8. ADO zapewnia bezpieczne przechowywanie danych osobowych przy użyciu nowoczesnego oprogramowania, które jest stale aktualizowane.

13.4.9. Dostęp do danych osobowych jest ograniczony do personelu, który potrzebuje dostępu i należy wprowadzić odpowiednie zabezpieczenia w celu uniknięcia nieupoważnionego udostępniania informacji.

13.4.10. Po usunięciu danych osobowych należy to zrobić w sposób bezpieczny, tak aby usunięcie danych było nieodwracalne.

13.4.11. Odpowiednie rozwiązania w zakresie kopii zapasowych i odzyskiwania danych zawiera Plan ciągłości działania stanowiący załącznik nr 12 do Polityki.

14. Naruszenia bezpieczeństwa ochrony danych

14.1. W przypadku naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych osobowych, ADO niezwłocznie, jednak nie później niż w ciągu 6 godzin, oceni ryzyko dla praw i wolności osób, a w razie potrzeby zgłosi to naruszenie PUODO - nie później niż 72 godziny po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Wzór zgłoszenia stanowi załącznik nr 9 do Polityki. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

14.2. Na każdym członku Personelu, który wiedział lub powinien wiedzieć o naruszeniu, ciąży obowiązek poinformowania ADO bądź IOD o tym naruszeniu, nie później niż w ciągu 6 godzin od powzięcia tej informacji.

14.3. Prowadzony jest rejestr incydentów – wzór stanowi załącznik nr 5 do Polityki, a także opis potencjalnych incydentów i sposoby postępowania – stanowi załącznik nr 6 do Polityki.

14.4. O naruszeniu należy bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą, jeśli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia jej praw lub wolności. Wzór zawiadomienia stanowi załącznik nr 9 do Polityki.

14.5. Zawiadomienie, o którym mowa w ust. 14.4., nie jest wymagane, w następujących przypadkach:

a) ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) ADO 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.

15. Wnioski o dostęp do informacji

15.1. Wszystkie osoby, które są przedmiotem danych osobowych będących w posiadaniu ADO, mają prawo do:

15.1.1. Zapytania, jakie informacje na ich temat ADO posiada i dlaczego.

15.1.2. Zapytania, jak uzyskać do nich dostęp.

15.1.3. Bycia informowanym, jak je aktualizować.

15.1.4. Bycia poinformowanym, w jaki sposób ADO spełnia swoje obowiązki w zakresie ochrony danych.

15.2. Jeśli dana osoba kontaktuje się z ADO i prosi o te informacje, nazywa się to żądaniem dostępu do informacji.

15.3. Wnioski o dostęp do informacji pochodzące od osób fizycznych powinny być wysyłane pocztą elektroniczną, zaadresowane do ADO na [adres e-mail]. ADO może zapewnić standardowy formularz wniosku, ale osoby, których dane dotyczą nie muszą się nim posłużyć, aby skorzystać z przysługującego im uprawnienia.

15.4. ADO zawsze zweryfikuje tożsamość osoby składającej wniosek o dostęp do podmiotu przed przekazaniem jakichkolwiek informacji.

15.5. ADO bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku jej wnioskiem.

15.6. Jeżeli ADO nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

16. Zgoda na przetwarzanie danych osobowych

16.1. ADO powinien pobierać zgody na przetwarzanie danych osobowych jedynie w sytuacjach, gdy nie znajduje zastosowania żadna inna podstawa przetwarzania danych osobowych, o której mowa w art. 6 i 9 RODO. W odniesieniu do niepełnoletnich uczniów zgodę w ich imieniu powinien wyrazić rodzic albo opiekun prawny.

16.2. W szczególności sytuacjami, w których ADO powinien uzyskać zgodę na przetwarzanie danych jest:

1) pobieranie danych dodatkowych, wykraczających poza katalog wynikający z przepisów,

2) wykonywanie działań, do których ADO nie znajduje umocowania w przepisach.

16.3. Jako przykłady sytuacji, o których mowa w ust. 16.2. należy podać:

a) rejestrację wizerunku ucznia, nauczyciela, a także pozostałych członków personelu i innych osób i publikację tego wizerunku na stronie internetowej placówki oraz na portalach społecznościowych (nie dotyczy monitoringu) – z zastrzeżeniem postanowień rozdziału 19.,

b) Zawieranie umów ubezpieczenia od następstw nieszczęśliwych wypadków (nie dotyczy zawierania umów ubezpieczenia w sytuacji, gdy placówka jest do tego

zobligowana przepisami, np. w przypadku organizowania wycieczek i wyjazdów zagranicznych),

c) Przetwarzanie danych osobowych w związku ze świadczeniem e-usług (nie dotyczy to usług, które placówka jest zobligowana na podstawie przepisów świadczyć w formie elektronicznej),

17. Monitoring i wizerunek

17.1. Jeżeli jest to niezbędne do zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony mienia osoba działająca w imieniu ADO, tj. dyrektor placówki, w uzgodnieniu z organem prowadzącym placówkę oraz po przeprowadzeniu konsultacji z radą pedagogiczną, radą rodziców i samorządem uczniowskim, może wprowadzić szczególny nadzór nad pomieszczeniami placówki lub terenem wokół placówki w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring).

17.2. Monitoring nie powinien stanowić środka nadzoru nad jakością wykonywania pracy przez Personel placówki.

17.3. Monitoring nie obejmuje pomieszczeń, w których odbywają się zajęcia dydaktyczne, wychowawcze i opiekuńcze, pomieszczeń, w których uczniom jest udzielana pomoc psychologiczno-pedagogiczna, pomieszczeń przeznaczonych do odpoczynku i rekreacji pracowników, pomieszczeń sanitarno-higienicznych, gabinetu profilaktyki zdrowotnej, szatni i przebieralni, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne ze względu na istniejące zagrożenie dla realizacji celu określonego w ust. 17.1. i nie naruszy to godności oraz innych dóbr osobistych uczniów, Personelu i innych osób, w szczególności zostaną zastosowane techniki uniemożliwiające rozpoznanie przebywających w tych pomieszczeniach osób.

17.4. Nagrania obrazu zawierające dane osobowe uczniów, Personelu i innych osób, których w wyniku tych nagrań można zidentyfikować, placówka przetwarza wyłącznie do celów, dla których zostały zebrane i przechowuje przez okres nie dłuższy niż 3 miesiące od dnia nagrania.

17.5. Po upływie okresu, o którym mowa w ust. 17.4., uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe uczniów, Personelu i innych osób, których w wyniku tych nagrań można zidentyfikować, podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej.

17.6. Dyrektor placówki informuje uczniów i Personel placówki o wprowadzeniu monitoringu, w sposób przyjęty w placówce, nie później niż 14 dni przed uruchomieniem monitoringu. Inne osoby znajdujące się w zasięgu monitoringu należy poinformować o tym fakcie w momencie ich wkroczenia na teren monitorowany. Ust. 19.8. stosuje się odpowiednio.

17.7. Dyrektor placówki przed dopuszczeniem osoby do wykonywania obowiązków służbowych informuje ją na piśmie o stosowaniu monitoringu.

17.8. W przypadku wprowadzenia monitoringu dyrektor placówki oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, a także realizuje obowiązek informacyjny za pomocą odpowiednich tablic, znaków lub ogłoszeń dźwiękowych, nie później niż dzień przed jego uruchomieniem.

17.9. Dyrektor placówki lub placówki, uzgadnia z organem prowadzącym placówka lub placówkę 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.

17.10. Możliwe jest rozpowszechnianie zdjęć z imprez, uroczystości, wycieczek w przypadku publikowania zdjęć, na których sylwetka osoby jest jedynie szczegółem całości uwiecznionej na zdjęciu. Aby zamieszczenie takiego zdjęcia reportażowego było możliwe bez uzyskania zgody, to:

a) osoba przedstawiona na zdjęciu nie może być głównym tematem fotografii, musi pojawić się na niej niejako „przy okazji", jako element uboczny,

b) dana osoba musi być elementem danego zdjęcia, szczegółem – zgromadzenia, krajobrazu, publicznej imprezy (wyliczenie jest przykładowe, może to być również wycieczka, impreza, uroczystość itd.),

c) zdjęcie nie powinno być zdjęciem pozowanym (pozowanie niejako oznaczałoby, że dana osoba jest jednak istotnym elementem zdjęcia, dopuszczalne jest jednak publikowanie zdjęć klasowych),

17.11. Dodatkowo, nawet w przypadku spełnienia powyższych zasad – zdjęcie w żaden sposób nie powinno naruszać prawa do prywatności przedstawionych na nim osób ani w żaden sposób naruszać ich dóbr osobistych.

17.12. Jeżeli nie zachodzą sytuacje wymienione w ust. 17.10. ADO powinien pobrać zgodę na utrwalenie i wykorzystanie wizerunku (wzór stanowi załącznik nr 11 do niniejszej Polityki).

18. Wykonywanie obowiązku informacyjnego

18.1. ADO zgodnie z art. 13 RODO ma obowiązek poinformować osobę, której dane przetwarza podczas pozyskiwania danych osobowych o:

18.1.1. swojej tożsamości i danych kontaktowych;

18.1.2. danych kontaktowych inspektora ochrony danych;

18.1.3. celach przetwarzania danych osobowych, oraz podstawie prawnej tego przetwarzania;

18.1.4. informacjach o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

18.1.5. gdy ma to zastosowanie – informacjach o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

18.1.6. okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

18.1.7. prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub

ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

18.1.8. jeżeli przetwarzanie odbywa się na podstawie zgody wyrażonej w oparciu art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO –o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

18.1.9. o prawie wniesienia skargi do organu nadzorczego;

18.1.10. tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

18.1.11. o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotnych informacjach o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

18.2. Jeżeli ADO pozyskuje dane w sposób pośredni od innych podmiotów oprócz informacji, o których mowa w ust. 18.1. należy podać zgodnie z art. 14 RODO:

- źródło pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych,
- kategorie danych osobowych, które są przetwarzane, a więc rodzaju przetwarzanych danych, np. imię, nazwisko, adres, data urodzenia, itd.

18.3. W praktyce realizacja obowiązku informacyjnego powinna przybrać formę przedstawienia osobie, której dane dotyczą w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, oświadczenia zawierającego informacje wymienione w ust. 18.1 oraz ewentualnie w 18.2. Oświadczenie może mieć formę np. pisemnego oświadczenia, wiadomości e-mail, tablicy informacyjnej, informacji na stronie internetowej, a uzależnione jest to od konkretnego przypadku i adresata tych informacji oraz od sytuacji, w której dane są pobierane. Jeśli jest to możliwe należy realizować obowiązek informacyjny w formie pisemnej z pisemnym potwierdzeniem osoby, której dane dotyczą o zapoznaniu się z informacją.

18.4. Wzór obowiązku informacyjnego stanowi załącznik nr 7 do Polityki. Niektóre elementy obowiązku mają charakter stały. Elementy, które trzeba dostosować do konkretnego przypadku i adresata tego obowiązku to: cel przetwarzania jego danych i podstawa prawna, czas przetwarzania danych, kategorie odbiorców danych, czy podanie danych jest obowiązkiem ustawowym, czy umownym. Pomocnym dokumentem będzie w tym przypadku Rejestr czynności przetwarzania, gdzie można znaleźć większość tych informacji. Propozycję wypełnionego obowiązku informacyjnego stanowi załącznik nr 8 do Polityki.

18.5. ADO powinien również poinformować osobę, której dane przetwarza, że ma zamiar przetwarzać dane w innym celu niż ten, w którym zostały zebrane, jeszcze zanim zacznie przetwarzać dane w nowym celu.

18.6. Ust. 20.1., 20.2., 20.5. nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.

19. Struktura dokumentacji

Poniżej znajduje się lista dokumentów, które ADO ma obowiązek utrzymywać. Od decyzji ADO zależy, czy dokumentacja będzie miała formę elektroniczną czy papierową. W sytuacji, gdy wymagane jest, aby osoba, do której kierowany jest określony dokument się z nim zapoznała i/lub wyraziła na zgodę na oświadczenie w nim zawarte, wówczas rekomendowane jest zachowanie papierowej formy w celach dowodowych.

Do dokumentacji wewnętrznej zaliczamy rejestr czynności przetwarzania, który jest rejestrem czynności przetwarzania danych osobowych, za które odpowiada ADO. Dokument ten musi zawierać elementy wskazane w art. 30 ust. 1 RODO.

W sytuacji, gdy ADO występuje również w charakterze podmiotu przetwarzającego powinien także prowadzić rejestr kategorii czynności przetwarzania. Dokument ten musi zawierać elementy wskazane w art. 30 ust. 2 RODO.

Sposoby technicznych zabezpieczeń stanowią listę rozwiązań, jakie zostały zastosowane, w celu zabezpieczenia przetwarzanych danych osobowych. Lista ta stanowi element rejestru czynności przetwarzania oraz oceny skutków dla ochrony danych.

19.1. LISTA OBOWIĄZKÓW WEWNĘTRZNYCH ADMINISTRATORA

19.1.1. Rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania (odrębne dokumenty)

19.1.2. Sposoby technicznych zabezpieczeń (element rejestru czynności przetwarzania i oceny skutków dla ochrony danych)

19.1.3. Ocena skutków dla ochrony danych (odrębny zestaw dokumentów)

19.1.4. Rejestr systemów – wzór (załącznik nr 1)

19.1.5. Powołanie IOD – wzór (załącznik nr 2)

19.1.6. Upoważnienie do przetwarzania danych i oświadczenie o zachowaniu tajemnicy – wzór (załącznik nr 3)

19.1.7. Ewidencja osób upoważnionych – wzór (załącznik nr 4)

19.1.8. Rejestr incydentów – wzór (załącznik nr 5)

19.1.9. Opis incydentów i sposoby postępowania (załącznik nr 6)

19.1.10. Obowiązek informacyjny – wzór (załącznik nr 7)

19.1.11. Obowiązek informacyjny – przykłady (załącznik nr 8)

19.1.12. Zgłoszenie w sprawie naruszenia ochrony danych osobowych (załącznik nr 9)

19.1.13. Zawiadomienie o naruszeniu ochrony danych osobowych (załącznik nr 10)

19.1.14. Zgoda na przetwarzanie wizerunku ucznia – wzór (załącznik nr 11)

19.1.15. Plan ciągłości działania (załącznik nr 12)

19.1.16. Zbiór głównych zasad przetwarzania danych osobowych (załącznik nr 13)

19.2. LISTA OBOWIĄZKÓW ZEWNĘTRZNYCH ADMINISTRATORA

19.2.1. Umowy powierzenia przetwarzania danych osobowych – wzór (załącznik nr 14)

Załącznik nr 2

Powołanie Inspektora Ochrony Danych

Z dniem …….. funkcję Inspektora Ochrony Danych w Zespole Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin) obejmuje

……

1. Inspektor ochrony danych posiada kwalifikacje zawodowe, a w szczególności wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań.
2. Administrator zapewnia, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
3. Administrator wspiera inspektora ochrony danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
4. Administrator zapewnia, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora.
5. Inspektor ochrony danych pełni funkcję punktu kontaktowego dla osób, których dane dotyczą wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw im przysługujących.
6. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.
7. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.
8. Inspektor ochrony danych ma w szczególności następujące zadania:
    a) informowanie ADO oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych i doradzanie im w tej sprawie;
    b) monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz polityk ADO w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z przepisami o ochronie danych osobowych

d) współpraca z organem nadzorczym;

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,

a także inne wynikające z Polityki ochrony danych ADO.

9. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

.....

w imieniu ADO

Załącznik nr 3

UPOWAŻNIENIE

do przetwarzania danych osobowych

w systemie informatycznym lub w zbiorze w wersji papierowej

Z dniem …….. upoważniam Panią/Pana ……

a) **do obsługi systemu informatycznego** Zespołu Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin) zgodnie z nadanymi uprawnieniami dostępowymi w zakresie niezbędnym do realizacji obowiązków służbowych na zajmowanym stanowisku lub zobowiązań umownych.

b) **do obsługi zbiorów danych osobowych w** Zespole Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin) **w wersji papierowej** zgodnie z zakresem obowiązków służbowych na zajmowanym stanowisku lub zobowiązań umownych.

Zobowiązuję Panią/Pana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych zasad ochrony danych osobowych zawartych w Polityce ochrony danych Zespołu Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin).

Niniejsze upoważnienie traci moc najpóźniej z dniem odwołania, rozwiązania lub wygaśnięcia umowy o pracę, umowy zlecenia, umowy o dzieło lub innego stosunku prawnego.

[miejsce i data],……. ……..

w imieniu ADO

OŚWIADCZENIE

Oświadczam, iż zostałam/em zapoznana/y z przepisami dotyczących ochrony danych osobowych, w szczególności 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 (ogólne rozporządzenie o ochronie danych), a także ustawy z dnia 24.05.2018 r. o ochronie danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych zasad ochrony danych osobowych zawartych w Polityce ochrony danych w Zespole Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin)

Zobowiązuję się do:

- zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zobowiązań umownych lub obowiązków pracowniczych,
- niewykorzystywania danych osobowych w celach pozasłużbowych i pozaumownych, o ile nie są one jawne,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne,
- korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych lub zobowiązań umownych,
- wykorzystywania jedynie legalnego oprogramowania pochodzącego od Administratora Danych Osobowych,
- należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją ochrony danych osobowych,
- korzystania z urządzeń przenośnych zgodnie z dokumentacją ochrony danych osobowych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Administratora danych osobowych za ciężkie naruszenie obowiązków pracowniczych lub zobowiązań umownych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy oraz Kodeksu Cywilnego lub za naruszenie przepisów karnych ww. ustawy o ochronie danych osobowych.

…….

podpis osoby upoważnionej

Załącznik nr 7

Obowiązek informacyjny zgodny z art. 13 ust. 1 RODO

(WZÓR)

1. Administratorem Państwa danych osobowych jest Zespół Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin). Z Administratorem można skontaktować się listownie: ul. Orawska 1, e-mailowo: zso3@miasto.um.pl.
2. Inspektorem Ochrony Danych jest […], z którym można się skontaktować […].
3. Państwa dane osobowe są przetwarzane w celu […] (**należy podać cel przetwarzania*), na podstawie […]. (**należy podać podstawę prawną przetwarzania np. art. 6 ust 1 pkt a/b/c/d/e RODO).*
4. Odbiorcami Państwa danych osobowych są: […] (**można wymienić kategorię odbiorców o ile istnieją*).
5. Państwa dane osobowe będą przechowywane przez okres […]. *(*jeżeli nie ma możliwości wskazania okresu przechowywania należy podać kryterium ustalania tego okresu np. do czasu wyłonienia zwycięscy konkursu, do czasu zakończenia rekrutacji itd.)*.
6. Mają Państwo prawo żądania od Administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do niesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
7. Jeżeli przetwarzanie odbywa się na podstawie zgody, mają Państwo prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
8. Mają Państwo prawo wnieść skargę do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych, jeśli uznają Państwo, iż przetwarzanie przez Administratora Państwa danych osobowych narusza przepisy dot. ochrony danych osobowych.
9. Podanie danych osobowych jest wymogiem *ustawowym / umownym / warunkiem zawarcia umowy. Są Państwo zobowiązani do podania danych (* jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania należy wskazać ewentualne konsekwencje niepodania danych)*.

Załącznik nr 8

OBOWIĄZEK INFORMACYJNY ZGODNY Z ART. 13 UST. 1 RODO

Klauzula informacyjna dla uczniów i rodziców – proces rekrutacji

1. Administratorem danych osobowych uczniów i rodziców jest Zespół Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin). Z Administratorem można skontaktować się listownie: ul. Orawska 1, e-mailowo: zso3@miasto.um.pl
2. Inspektorem Ochrony Danych jest […], z którym można się skontaktować […].
3. Dane osobowe są przetwarzane w celu przeprowadzenia rekrutacji do [...] , na podstawie:
   a) art. 6 ust. 1 lit. c RODO, a dokładnie w celu wykonania obowiązku prawnego nałożonego art. 13/14 oraz art. 130 i nast. ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz.U. z 2017 r., poz., 59 ze zm.),
   b) art. 9 ust. 2 lit. h RODO.
4. Odbiorcami danych osobowych są upoważnieni pracownicy Administratora, podmioty, którym należy udostępnić dane osobowe na podstawie przepisów prawa, a także te, którym dane zostaną powierzone do zrealizowania celów przetwarzania.
5. Dane osobowe pozyskane w procesie rekrutacji będą przechowywane nie dłużej niż do końca okresu, w którym uczeń będzie uczęszczał będzie do placówki, a w przypadku nieprzyjęcia do placówki – przez okres jednego roku.
6. Mają Państwo prawo żądania od Administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do niesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
7. Mają Państwo prawo wnieść skargę do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych, jeśli uznają Państwo, iż przetwarzanie przez Administratora Państwa danych osobowych narusza przepisy dot. ochrony danych osobowych.
8. Podanie danych osobowych jest wymogiem ustawowym. W celu uczestniczenia w rekrutacji są Państwo zobowiązani do podania danych. Niepodanie danych skutkuje odmową uczestnictwa w rekrutacji.

Klauzula informacyjna dla uczniów i rodziców – po przyjęciu

1. Administratorem danych osobowych uczniów i rodziców jest Zespół Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin). Z Administratorem można skontaktować się listownie: ul. Orawska 1, e-mailowo: zso3@miasto.um.pl
2. Inspektorem Ochrony Danych jest […], z którym można się skontaktować […].
3. Dane osobowe są przetwarzane na podstawie:

a) art. 6 ust. 1 lit. a i art. 9 ust. 2 lit. a RODO, tj. na podstawie zgody udzielonej w celach określonych każdorazowo w przekazywanych formularzach zgody, w tym w celu promowania działalności placówki oraz osiągnięć i umiejętności ucznia, a także w celu zapewnienia udziału w zajęciach dodatkowych, korzystania z e-usług […], żywienia uczniów, korzystania z pomocy psychologiczno-pedagogicznej, zawarcia umowy ubezpieczenia NNW;

b) art. 6 ust. 1 lit. c RODO, tj. gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na placówce, w tym w związku z realizacją celów dydaktycznych, wychowawczych i opiekuńczych placówki w celu wykonania obowiązków prawnych nałożonych art. 13/14 ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz.U. z 2017 r., poz., 59) takich, jak prowadzenie ewidencji uczniów na potrzeby procesów nauczania, realizacja procesu nauczania, prowadzenie dziennika lekcyjnego, prowadzenie zadań z zakresu opieki pielęgniarskiej, żywienie uczniów, prowadzenie zajęć dodatkowych, realizacja zadań z zakresu BHP, wypożyczanie książek z biblioteki szkolnej, prowadzenie świetlicy szkolnej;

c) art. 6 ust. 1 lit. f RODO, tj. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez placówkę, w tym w związku ze stosowaniem monitoringu w celu zapewnienia bezpieczeństwa uczniów, pracowników i mienia placówki, prowadzeniem prac konserwatorskich i napraw infrastruktury informatycznej;

d) Art. 9 ust. 2 lit. h RODO w celu świadczenia opieki pielęgniarskiej i profilaktyki zdrowia uczniów, prowadzenia ewidencji uczniów na potrzeby procesów nauczania, realizacji procesu nauczania, realizacji zadań z zakresu BHP.

4. Prawnie uzasadnione interesy realizowane przez Administratora w związku z przetwarzaniem danych to zapewnienie bezpieczeństwa uczniów i pracowników, a także ochrony mienia placówki oraz zapewnienie prawidłowego funkcjonowania infrastruktury informatycznej w szkole

5. Odbiorcami danych osobowych są upoważnieni pracownicy Administratora, podmioty, którym należy udostępnić dane osobowe w celu wykonania obowiązku prawnego, a także podmioty, którym dane zostaną powierzone do zrealizowania celów przetwarzania.

6. Dane osobowe będą przechowywane co najmniej do końca okresu, w którym uczeń będzie uczęszczał do placówki lub do czasu wycofania zgody, zgłoszenia sprzeciwu, a w każdym razie przez okres wskazany przepisami związanymi z wypełnianiem obowiązku prawnego przez placówkę.

7. Mają Państwo prawo żądania od Administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.

8. W przypadku danych przetwarzanych na podstawie zgody, mają Państwo prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

9. Mają Państwo prawo wnieść skargę do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych, jeśli uznają Państwo, iż przetwarzanie przez Administratora Państwa danych osobowych narusza przepisy dot. ochrony danych osobowych.

10. Podanie danych osobowych w celu wykonania przez Administratora obowiązku prawnego jest wymogiem ustawowym. W celu uczęszczania ucznia do placówki są Państwo zobowiązani do podania danych. Niepodanie danych skutkuje niemożnością realizowania zadań przez placówkę względem ucznia. Podanie danych udostępnionych na podstawie zgody jest dobrowolne, a brak zgody spowoduje niemożność zrealizowania zamierzonego celu, lecz nie wpłynie na realizację głównych zadań przez placówkę względem ucznia.

Klauzula informacyjna dla kandydatów do pracy

1. Administratorem Państwa danych osobowych jest Zespół Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin). Z Administratorem można skontaktować się listownie: ul. Orawska 1, e-mailowo: zso3@miasto.um.pl
2. Inspektorem Ochrony Danych jest […], z którym można się skontaktować […].
3. Państwa dane kontaktowe są przetwarzane w celu przeprowadzenia rekrutacji na stanowisko pracownicze do [...] , na podstawie:
   a) art. 6 ust. 1 lit. c RODO tj. gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na placówce, w tym w związku z wykonaniem obowiązków nałożonych art. 22 (1) par. 1 Kodeksu Pracy, art. 10 ust. 5 Karty Nauczyciela, art. 13/14 ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz.U. z 2017 r., poz., 59)
   b) art. 6 ust. 1 lit. a RODO tj. na podstawie zgody udzielonej w celach określonych każdorazowo w przekazywanych formularzach zgody,
   c) art. 6 ust. 1 lit. b RODO - podjęcie działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.
4. Odbiorcami danych są upoważnieni pracownicy Administratora, podmioty, którym należy udostępnić dane osobowe w celu wykonania obowiązku prawnego, a także podmioty, którym dane zostaną powierzone do zrealizowania celów przetwarzania.
5. Państwa dane osobowe będą przechowywane do zakończenia procesu rekrutacji, chyba że wyrażą Państwo zgodę na ich przetwarzanie na potrzeby dalszych procesów rekrutacyjnych.
6. Mają Państwo prawo żądania od Administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do niesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
7. W przypadku danych przetwarzanych na podstawie zgody, mają Państwo prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
8. Mają Państwo prawo wnieść skargę do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych, jeśli uznają Państwo, iż przetwarzanie przez Administratora Państwa danych osobowych narusza przepisy dot. ochrony danych osobowych.
9. Podanie danych osobowych jest dobrowolne, ale w celu uczestniczenia w rekrutacji są Państwo zobowiązani do podania danych. Niepodanie danych skutkuje odmową uczestnictwa w rekrutacji.

Klauzula informacyjna dla pracowników

1. Administratorem Państwa danych osobowych jest Zespół Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin). Z Administratorem można skontaktować się listownie: ul. Orawska 1, e-mailowo: zso3@miasto.um.pl

2. Inspektorem Ochrony Danych jest […], z którym można się skontaktować […].

3. Państwa dane kontaktowe są przetwarzane w celu nawiązania stosunku pracy, prowadzenia ewidencji pracowników zgodnie z Kodeksem Pracy, zgłoszenia pracownika i członków jego rodziny do ZUS, ich aktualizacji oraz przekazywania informacji o zwolnieniach, prowadzenia rozliczeń z pracownikami i realizacji innych świadczeń pracowniczych, naliczania potrąceń, obliczania składek ZUS, na podstawie:

   a) art. 6 ust. 1 lit. c i art. 9 ust. 2 lit. b RODO tj. gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na placówce oraz przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, w tym w związku z wykonaniem obowiązków nałożonych art. 22 (1) par. 1 i 2 Kodeksu Pracy, art. 10 ust. 5 Karty Nauczyciela, art. 13/14 ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz.U. z 2017 r., poz., 59), art. 1, 6 oraz 6a ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych,

   b) art. 6 ust. 1 lit. a RODO tj. na podstawie zgody udzielonej w celach określonych każdorazowo w przekazywanych formularzach zgody,

   c) art. 6 ust. 1 lit. b RODO - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą.

4. Odbiorcami danych są upoważnieni pracownicy Administratora, podmioty, którym należy udostępnić dane osobowe w celu wykonania obowiązku prawnego, a także podmioty, którym dane zostaną powierzone do zrealizowania celów przetwarzania.

5. Państwa dane osobowe będą przechowywane przez 50 lat od ustania stosunku pracy.

6. Mają Państwo prawo żądania od Administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.

7. W przypadku danych przetwarzanych na podstawie zgody, mają Państwo prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

8. Mają Państwo prawo wnieść skargę do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych, jeśli uznają Państwo, iż przetwarzanie przez Administratora Państwa danych osobowych narusza przepisy dot. ochrony danych osobowych.

9. Podanie danych osobowych jest wymogiem ustawowym - są Państwo zobowiązani do podania danych. Niepodanie danych skutkuje odmową nawiązania stosunku pracy.

Klauzula informacyjna dla osób znajdujących się w zasięgu monitoringu

1. Administratorem Państwa danych osobowych jest Zespół Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin). Z Administratorem można skontaktować się listownie: ul. Orawska 1, e-mailowo: zso3@miasto.um.pl
2. Inspektorem Ochrony Danych jest […], z którym można się skontaktować […].
3. Dane osobowe są przetwarzane w celu prowadzenia działań w zakresie zachowania bezpieczeństwa i porządku w placówce, na podstawie art. 6 ust. 1 lit. f RODO.
4. Prawnie uzasadnione interesy realizowane przez Administratora to zapewnienie bezpieczeństwa uczniów i pracowników, a także ochrony mienia placówki.
5. Odbiorcami danych są upoważnieni pracownicy Administratora, podmioty, którym należy udostępnić dane osobowe w celu wykonania obowiązku prawnego, a także podmioty, którym dane zostaną powierzone do zrealizowania celów przetwarzania.
6. Dane osobowe pozyskane w drodze monitoringu będą przechowywane do 3 miesięcy od dnia nagrania.
7. Mają Państwo prawo żądania od Administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do niesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
8. Mają Państwo prawo wnieść skargę do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych, jeśli uznają Państwo, iż przetwarzanie przez Administratora Państwa danych osobowych narusza przepisy dot. ochrony danych osobowych.
9. Podanie danych osobowych jest obowiązkowe. Niepodanie danych skutkuje odmową wstępu na teren placówki.

Załącznik nr 9

……..

(miejscowość, data)

Administrator danych

.....

Urząd Ochrony Danych Osobowych

ul. Stawki 2

00-193 Warszawa

ZGŁOSZENIE

W SPRAWIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Niniejszym w trybie art. 33 ogólnego rozporządzenia o ochronie danych, zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu … w … .

1.	**Charakter naruszenia ochrony danych:**	Np. *Przesłanie przez pracownika wiadomości e-mail do błędnego adresata (nieznana osoba) zamiast do współpracownika wraz z załącznikiem w formacie pliku Excel (niezabezpieczonego) zawierającego dane rodziców i uczniów (takie jak: imię i nazwisko, adres zamieszkania, PESEL, nr. dowodu tożsamości,, numer telefonu, adresy e-mail)*
2.	**Kategoria i przybliżona liczba osób, których dane dotyczą:**	Np. *Wychowankowie, rodzice. Liczba osób, których dane dotyczą .....*
3.	**Liczba wpisów, których dotyczy naruszenie:**	Np. *821*

4.	**Możliwe konsekwencje naruszenia ochrony danych:**	Np. *Powstanie szkód majątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub kradzież lub sfałszowanie tożsamości, strata finansowa*
5.	**Środki zastosowane lub proponowane w celu zaradzenia naruszenia ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:**	Np. *Wdrożenie stosownych środków kryptograficznych, w tym w tym pseudonimizacja, zakaz przesyłania załączników zawierających dane osobowe w sposób niezabezpieczony.*
6.	**Dane inspektora ochrony danych**	Np. *....., nr. telefonu: XXX XXX XXX, adres e-mail: iod@domena.pl*

……
…….*

……

(podpis dyrektora)

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

Załącznik nr 10

……..

(miejscowość, data)

Administrator danych

.....

Adresat

…….

ZAWIADOMIENIE

O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Niniejszym w trybie art. 34 ogólnego rozporządzenia o ochronie danych, zawiadamiam o naruszeniu ochrony danych osobowych, które miało miejsce w dniu … w … .

1.	**Charakter naruszenia ochrony danych:**	Np. *Przesłanie przez pracownika wiadomości e-mail do błędnego adresata (nieznana osoba) zamiast do współpracownika wraz z załącznikiem w formacie pliku Excel (niezabezpieczonego) zawierającego dane rodziców i uczniów (takie jak: imię i nazwisko, adres zamieszkania, PESEL, nr. dowodu tożsamości,, numer telefonu, adresy e-mail)*
2.	**Możliwe konsekwencje naruszenia ochrony danych:**	Np. *Powstanie szkód majątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub kradzież lub sfałszowanie tożsamości, strata finansowa*
3.	**Środki zastosowane lub proponowane w celu zaradzenia**	Np. *Wdrożenie stosownych środków kryptograficznych, w tym w tym pseudonimizacja, zakaz przesyłania*

	naruszenia ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:	*załączników zawierających dane osobowe w sposób niezabezpieczony.*
4.	**Dane inspektora ochrony danych**	Np. ....., *nr. telefonu: XXX XXX XXX, adres e-mail: iod@domena.pl*

……
…….*

……

(podpis dyrektora)

Załącznik nr 11

……, dn. ……

(miejscowość) *(data)*

…….

(imię i nazwisko rodzica lub opiekuna prawnego)

ZGODA NA PRZETWARZANIE I WYKORZYSTANIE WIZERUNKU UCZNIA

1. Na podstawie art. 6 ust. 1 lit. a 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 (ogólne rozporządzenie o ochronie danych) **wyrażam zgodę** na przetwarzanie przez Zespół Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin) wizerunku mojego dziecka …….. *(podać imię i nazwisko dziecka)* poprzez jego publikację na stronie internetowej placówki i na jej profilu na portalu Facebook w celu promowania działalności placówki oraz osiągnięć i umiejętności dziecka.

2. Na podstawie art. 81 ustawy o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r. (tekst jedn.: Dz.U. z 2017 r., poz. 880 ze zm.) **wyrażam zgodę** na nieodpłatne wykorzystanie wizerunku mojego dziecka…… (*podać imię i nazwisko dziecka*) przez Zespół Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin) w postaci zdjęć i materiałów filmowych, zarejestrowanego w ramach zajęć przedszkolnych, wycieczek, konkursów, wyjść, uroczystości i innych wydarzeń organizowanych przez Zespół Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin). Zgoda obejmuje zamieszczanie zdjęć i filmów na stronie internetowej placówki i na jej profilu na portalu Facebook w celu promowania działalności placówki oraz osiągnięć i umiejętności dziecka.

……..

(czytelny podpis rodzica lub opiekuna prawnego)

Załącznik nr 12

PLAN CIĄGŁOŚCI DZIAŁANIA WRAZ Z WYKAZEM STOSOWANYCH ZABEZPIECZEŃ

W tej procedurze opisano, w jaki sposób tworzone są kopie zapasowe jednostek (komputerów, serwerów) centrów danych i na jakich obszarach, w jaki sposób można przywrócić pliki oraz w jaki sposób można odzyskać pliki w przypadku niedostępności podstawowego centrum danych.

Odpowiedzialność w tym zakresie ponosi kierownik organizacyjno-gospodarczy oraz personel IT.

Personel IT odpowiedzialny jest za:

1) Utrzymywanie serwerów z kopią zapasową.

2) Ocena procesu tworzenia kopii zapasowej, przywracania i odzyskiwania co najmniej raz w roku.

3) Pomoc w rozwiązywaniu problemów z błędami kopii zapasowej na poziomie aplikacji.

4) Administrowanie bazową infrastrukturą pamięci masowej.

Kopie zapasowe danych przesyłane są na serwer szkoły, a następnie kopiowane na dysk przenośny, który przechowuje się w szkolnym sejfie znajdujący się w księgowości. Dane zabezpieczone są 24 x 7, a dostęp jest zapewniany wyłącznie uprawnionemu personelowi.

Szkoła stosuje rozwiązanie, które chroni wszystkie dane i sprawia, że są one łatwo dostępne, niezależnie od tego, czy są to pliki IT, bazy danych czy systemy pocztowe. Struktura kopii zapasowej powoduje, że dane są dostępne w dwóch kopiach. W przypadku błędów związanych z nośnikami i / lub dyskami zapewnia to, że utrata danych w systemie zapasowym jest niemożliwa i chroni przed utratą danych w przypadku awarii, w której utracono wszystkie kopie pierwotne.

System wykorzystuje szyfrowanie danych. Szyfrowanie odbywa się za pomocą oprogramowania do tworzenia kopii zapasowych; stąd dane są wysyłane i przechowywane w postaci zaszyfrowanej. Ponadto szyfrowanie Blowfish jest wykorzystywane jako standard.

Przywracanie wykonuje personel IT z zabezpieczonych nośników.

Załącznik nr 13

ZBIÓR GŁÓWNYCH ZASAD PRZETWARZANIA DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ OGÓLNOKSZTAŁCĄCYCH NR 3 (ul. Orawska 1, 70-131 Szczecin)

I. Zasady korzystania z internetu

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody w infrastrukturze IT spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo ze względu na zainstalowane na nich szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem.
5. Zabrania się w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą https://. W tej sytuacji należy „kliknąć" na ikonę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.

II. Procedura rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany sprawdzić jest urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

2. W celu rozpoczęcia pracy w systemie informatycznym użytkownik

e) loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła

3. Niedopuszczalne jest uwierzytelnianie się na hasło i identyfikator innego użytkownika lub praca w systemie informatycznym na koncie innego użytkownika.

4. Podczas nieobecności przy stanowisku komputerowym należy wylogować się z systemu.

5. Ekrany monitorów na stanowiskach, przy których przetwarza się dane osobowe, powinny być ustawione w sposób uniemożliwiający dostęp osób nieupoważnionych do informacji na nich wyświetlanych oraz konieczne jest stosowanie wygaszacza ekranu.

6. Zakończenie pracy użytkownika w systemie następuje po wylogowaniu się z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności dokumenty i wydruki zawierające dane osobowe, przed dostępem osób nieupoważnionych.

7. Nośniki komputerowe na których znajdują się ważne dane (w tym dane osobowe) powinny być oznaczone w sposób trwały, jednoznaczny i czytelny oraz przechowywane w szafie zamykanej na klucz.

III. Zasady użytkowania komputerów przenośnych

1. Każdy Użytkownik komputera przenośnego winien zapoznać się z zasadami użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.
2. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Pracodawcy, Użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8- znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).
3. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Pracodawcy.
4. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych tj. ADO lub IOD, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
   1) zaleca się przenoszenie go w specjalnym futerale;
   2) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru;
   3) podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod tylnym siedzeniem kierowcy.
6. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp.
7. Komputery przenośne po zakończeniu pracy przechowuje się wyłącznie w szafkach zamykanych na klucz.
8. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
9. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

IV. Zasady wynoszenia nośników z danymi osobowymi poza szkołę

1. Użytkownicy nie mogą wynosić poza szkołę bez zgody Administratora danych żadnych wymiennych elektronicznych nośników informacji, tj. wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash.

2. W sytuacjach koniecznych, za zgodą Administratora danych, wynoszone nośniki wymienne muszą być zaszyfrowane, a pliki opatrzone hasłem.

3. Pracownikom nie wolno wynosić poza szkołę dokumentacji papierowej, zwierającej dane osobowe (dzienniki, arkusze ocen). W przypadku innej dokumentacji (prace klasowe, listy uczestników wycieczek, dokumentacja wycieczek) należy ją przenosić w zamykanych teczkach lub w innej bezpiecznej formie.

4. W przypadku przesyłania dokumentacji j/w należy korzystać z zaufanych firm kurierskich, za pokwitowaniem i w opakowaniach gwarantujących niedostępność osób trzecich.

V. Zabezpieczenie danych w systemie informatycznym

1. System informatyczny zabezpiecza się :

   a) przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do tego systemu poprzez stosowanie specjalistycznego oprogramowania

   b) utratą danych spowodowaną awarią lub zakłóceniami w sieci zasilającej

2. System informatyczny służący do przetwarzania danych osobowych jest zabezpieczony przed utratą danych spowodowanych awarią zasilania lub zakłóceniami w sieci zasilającej poprzez stosowanie :

   a) agregatów awaryjnych UPS, które znajdują się w gabinecie dyrektora i wicedyrektora sekretariacie, księgowości

   b) listew przepięciowych, połączonych pomiędzy siecią zasilającą a komputerami

3. W celu ochrony systemów przed szkodliwym oprogramowaniem - oprogramowanie antywirusowe podlegające systematycznej aktualizacji musi być zainstalowane na każdym stanowisku komputerowym.

4. W szkole stosuje się aktywną ochronę antywirusową na każdym komputerze, na którem przetwarzane są dane osobowe.

5. Użytkownicy systemu są odpowiedziani za nieudostępnianie stanowisk pracy osobom postronnym.

VI. Zasady zabezpieczania dokumentacji papierowej z danymi osobowymi

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**”. Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.

2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.

3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. na korytarzach, kserokopiarkach, drukarkach oraz w pomieszczeniach ogólnodostępnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np. na terenach publicznych miejskich.

VII. Zasady tworzenia kopii zapasowych

1. Zbiory danych osobowych w systemie informatycznych są zabezpieczane przed utratą lub uszkodzeniem za pomocą:
    1) urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
    2) sporządzania kopii zapasowych (kopie pełne).
2. Pełne kopie zapasowe zbiorów danych tworzone są 2 razy w ciągu roku. Kopie systemu kadrowo płacowego całościowe sporządzane są raz w miesiącu, a kopie przyrostowe raz dziennie.
3. W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania lub systemu należy wykonać bezwzględnie pełną kopię zapasową systemu.
4. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzenie tych czynności odpowiada wyznaczony pracownik.
5. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.
6. Kopie całościowe przechowywane są przez 5 lat a kopie przyrostowe przez 1 miesiąc.

VIII. Procedura niszczenia danych na nośnikach elektronicznych

1. W odniesieniu do nośników przenośnych oraz nośników danych zainstalowanych w komponentach informatycznych – złomowanych stosowane są mechanizmy bezpiecznego kasowania informacji:
    1) za pomocą specjalistycznego oprogramowania;
    2) przy użyciu demagnetyzacji;
    3) poprzez fizyczne niszczenie (pocięcie, spalenie) nośników;
2. ADO lub IDO dokonuje kontroli prawidłowości usunięcia informacji.
3. Nośniki usuwalne, które nie mogą być ponownie wykorzystane, są niszczone.
4. Za właściwe skasowanie informacji zawartej na nośniku przenośnym lub w pamięci masowej stacji roboczej odpowiada użytkownik.
5. Za kasowanie informacji z pamięci masowych serwerów oraz nośników kopii archiwalnych i zapasowych odpowiada administrator danych.
6. Niszczenie nośnika zostaje odnotowane w protokole zniszczenia.

IX. Procedura niszczenia danych na nośnikach papierowych

Dokumentacja papierowa niszczona jest w niszczarkach paskowych oraz w niszczarkach o podwyższonym standardzie.

X. Procedura napraw w serwisach zewnętrznych

1. Komputery przeznaczone do naprawy należy wysyłać bez dysków a urządzenia mobilne bez kart pamięci.
2. W przypadku naprawy sprzętu z danymi osobowymi na nośniku należy je trwale usunąć z użyciem specjalistycznego oprogramowania.
3. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podawania hasła.
5. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site)

Załącznik nr 14

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:

Zespołem Szkół Ogólnokształcących Nr 3 (ul. Orawska 1, 70-131 Szczecin)

zwaną w dalszej części umowy „Administratorem”

reprezentowaną przez:

[…]

oraz

[…]

zwaną w dalszej części umowy „Podmiotem przetwarzającym”

reprezentowaną przez:

[…]

§ 1

Powierzenie przetwarzania danych osobowych

1. Administrator powierza Podmiotowi przetwarzającemu dane osobowe w trybie art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (zwanego w dalszej części „RODO”) do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi RODO.

§2

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał powierzone na podstawie umowy dane klientów Administratora w postaci m.in.: imienia i nazwiska, firmy (nazwy); adresu korespondencyjnego; numeru rachunku bankowego; numeru telefonu; adresu e-mail; NIP-u; REGON-u; PESEL-u.
2. Na powyższych danych będą wykonywane operacje: zbierania, utrwalania, organizowania, porządkowania, przechowywania, adaptowania lub modyfikowania,

pobierania, przeglądania, wykorzystywania, ujawniania poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie w rozumieniu art. 4 pkt. 2 RODO (*należy wybrać rodzaj operacji do których Podmiot przetwarzający będzie uprawniony).

§3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba, że obowiązek taki nakłada na nich prawo UE lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający poinformuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
2. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 RODO.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b RODO) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca *(*niepotrzebne skreślić)* Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 RODO.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi, nie później niż w ciągu 24 h.
8. Podmiot przetwarzający udostępni Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwi Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji – na zasadach określonych w niniejszej Umowie, i przyczyni się do nich.

§ 4

Prawa Administratora

1. Administrator zgodnie z art. 28 ust. 3 pkt h) RODO ma prawo dokonania audytu, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
2. Administrator dokona audytu w godzinach pracy Podmiotu przetwarzającego a Podmiot przetwarzający weźmie w nim konstruktywny udział.
3. Audyt dotyczyć będzie przetwarzania danych na mocy umowy głównej w celu wskazania zgodności z obowiązkami przewidzianymi w art. 28 RODO.
4. Warunkiem przeprowadzenia audytu jest zawiadomienie Podmiotu przetwarzającego w terminie nie krótszym niż 14 dni przed planowanym terminem jego przeprowadzenia.
5. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO.
6. Administratorowi przysługuje prawo kierowania zapytań do Podmiotu przetwarzającego w zakresie prawidłowości wykonania obowiązków dotyczących zabezpieczenia powierzonych mu na podstawie niniejszej Umowy danych. Podmiot przetwarzający zobowiązuje się udzielić odpowiedzi na zapytanie w terminie 14 dni od daty wpłynięcia zapytania.
7. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas audytu w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.
8. Jeżeli Podmiot przetwarzający podzleca obowiązki wynikające z niniejszej Umowy, musi uwzględnić prawa dotyczące audytów w Umowie zawartej z podwykonawcą, aby umożliwić Administratorowi efektywne audytowanie zgodności.

§5

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom po uzyskaniu uprzedniej szczegółowej bądź ogólnej pisemnej zgody Administratora.
2. Podwykonawca, o którym mowa w §4 ust. 1 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
3. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym

lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§7

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony* od ….. do ….. .*
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem …… * okresu wypowiedzenia.

§8

Rozwiązanie umowy

1. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot 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 bez zgody Administratora danych.

§9

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy prawa polskiego oraz RODO.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie właściwy rzeczowo sąd w […].

_____ _____

Administrator Podmiot przetwarzający