Polityka ochrony danych osobowych.

Wydanie 2.

Szkoła Podstawowa w Romanowie Dolnym

18 IX 2019 r.

Cel:
Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

Podstawy prawne:

1. rozporządzenie Parlamentu Europejskiego i Rady Europy (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 (RODO) (4.5.2016, L 119)
2. ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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) (Dz. U. 2019 poz. 730)
3. ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz.U. 2018 r., poz. 1000 z późn. zm.).

Przedmiot:
Przedmiotem Polityki ochrony danych osobowych są zasady i tryb postępowania podczas przetwarzania danych osobowych w formie tradycyjnej i elektronicznej. Mając na względzie obowiązek stosowania odpowiednich zabezpieczeń przetwarzanych danych osobowych w odniesieniu do zakresu, kontekstu i celu, a także ryzyka naruszenia ochrony przetwarzanych danych, zgodnie z art. 32 RODO, wdraża się odpowiednie środki techniczne i organizacyjne.

Zakres stosowania:

Polityka ochrony danych osobowych obowiązuje wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy informacyjne, w których przetwarzane są dane osobowe. Politykę tę stosuje się we wszystkich lokalizacjach, w których przetwarzane są informacje podlegające ochronie, na wszystkich nośnikach informacji (tradycyjnych - papierowych, elektronicznych, optycznych, magnetycznych), które zawierają dane podlegające ochronie. Polityka obowiązuje wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, w tym stażystów i osób, z którymi podpisane są umowy cywilno-prawne wykonujących prace na rzecz Administratora oraz innych osób mających dostęp do danych.

ZATWIERDZAM I POLECAM STOSOWAĆ

……..

Kierownik Jednostki

SPIS TREŚCI

DEFINICJE

Ilekroć w niniejszej Polityce jest mowa o:

1) Administratorze danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, które decydują o celach i środkach przetwarzania danych osobowych, a w niniejszej Polityce Dyrektorze Szkoły Podstawowej im. 67 Pułku Piechoty w Romanowie Dolnym, Romanowo Dolne 12, 464 – 700 Czarnków - Kierownika Jednostki zwanego „Administratorem”;
2) Inspektor Ochrony Danych (lub IDO) – rozumie się przez to osobę wyznaczoną przez Administratora, która jest odpowiedzialna za zapewnienie przetwarzania danych zgodnie z odpowiednimi przepisami prawa;
3) Administratorze Systemów Informatycznych (lub ASI) – rozumie się przez to osobę wyznaczoną przez Administratora, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane osobowe spełniały wymagania przewidziane przepisami prawa;
4) Danych osobowych (lub danych) – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5) Osobie upoważnionej – rozumie się przez to osobę, która otrzymała od Administratora pisemne upoważnienie do przetwarzania danych;
6) Przetwarzaniu danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych;
7) Upoważnieniu – rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska oraz stanowiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu;
8) RODO - 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 – RODO);
9) PUDO lub Urząd nadzoru – Prezes Urzędu Ochrony Danych Osobowych;
10) Zbiorze danych – rozumie się przez to dane zebrane w postaci zbioru lub według kategorii:
    a) danych osobowych uczniów SP w Romanowie Dolnym z podzbiorami,
    b) danych pracowniczych z podzbiorami,
    c) danych administracyjnych z podzbiorami,
    d) danych doraźnych,

przy czym każdy zbiór danych to zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

POSTANOWIENIA OGÓLNE

§ 1.

Przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

1. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem, co nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

INSPEKTOR DANYCH OSOBOWYCH I ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

§ 2.

1. Administrator wyznacza i zgłasza do rejestru prowadzonego przez Urząd nadzoru Inspektora Ochrony Danych, który jest odpowiedzialny za przetwarzanie danych.
2. Administrator wyznacza Administratora Systemów Informatycznych
3. Administrator wyznacza osoby współdziałające z IDO w zakresie ochrony danych osobowych.

§ 3.

W przypadku niewyznaczenia IDO lub ASI za zapewnienie należytego przestrzegania zasad ochrony danych osobowych odpowiada Administrator.

§ 4.

1. W przypadku powzięcia jakichkolwiek wątpliwości co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do IDO z wnioskiem o rozstrzygnięcie wątpliwości.
2. Przed udzieleniem przez IDO odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie danych osobowych i ich utrwalanie, a w przypadku posiadania już danych osobowych których wątpliwość dotyczy należy, do czasu rozstrzygnięcia wątpliwości, wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości czy są prawnie uzasadnione.

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 5.

Do przetwarzania danych osobowych w SP w Romanowie Dolnym są dopuszczone wyłącznie osoby upoważnione przez Administratora.

§ 6.

1. Upoważnienia nadawane są indywidualnie, przed rozpoczęciem przez osobę upoważnianą przetwarzania danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych mogą uzyskać wyłącznie pracownicy oraz osoby fizyczne współpracujące z Administratorem, które uzyskują dostęp do danych osobowych w związku ze świadczeniem na jego rzecz usług na podstawie umów cywilnoprawnych lub jako osoby fizyczne wykonujące obowiązki na podstawie jednoosobowej działalności (zatrudnieni).
3. Upoważnienie nadawane jest niezwłocznie po przyjęciu do pracy lub po zawarciu umowy cywilnoprawnej, w sytuacjach gdy zakres wykonywanych obowiązków wiąże się z potrzebą uzyskania dostępu do danych osobowych.
4. Upoważnienie nadawane jest na czas zatrudnienia na danym stanowisku pracy lub na czas realizacji zleconych czynności.
5. Upoważnienie do przetwarzania danych osobowych nadawane jest przez Administratora.
6. Osoba posiadająca upoważnienie do przetwarzania danych jest uprawniona do ich przetwarzania w zakresie i czasie wskazanym w upoważnieniu.
7. Inspektor Danych Osobowych na podstawie wydanych upoważnień prowadzi ewidencję (rejestr) osób upoważnionych do przetwarzania danych.
8. Każda osoba upoważniana do przetwarzania danych osobowych składa pisemne oświadczenie o zachowaniu w tajemnicy przetwarzanych danych osobowych oraz znanych jej informacji o stosowanych wobec danych środkach bezpieczeństwa.
9. Zatrudnieni, którzy w ramach swoich obowiązków przebywają w strefach gdzie przetwarzane są dane osobowe ale do ich obowiązków nie należy przetwarzanie danych osobowych muszą uzyskać przeszkolenie w zakresie ochrony danych osobowych i złożyć stosowne oświadczenie o przestrzeganiu zasad ochrony danych oraz zachowaniu tajemnicy.

§ 7.

1. Każdy kto przetwarza dane osobowe obowiązany jest zachować w tajemnicy dane osobowe do których posiada dostęp zarówno zamierzony jak i przypadkowy, sposoby zabezpieczania danych jak również wszelkie informacje, które powzięły w czasie przetwarzania danych. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
2. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.
3. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się, czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.

4. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać w innym środkiem komunikacji elektronicznej.

§ 8.

1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do osoby małoletniej – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
2. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą, Administrator jest obowiązany spełnić obowiązek informacyjny, wobec osoby, której dane uzyskano bezpośrednio po utrwaleniu zebranych danych.
3. Powyższy obowiązek Administrator nakłada na osoby zatrudnione przy przetwarzaniu danych osobowych, zobowiązując je do jego należytego wykonywania zgodnie z treścią dokumentów (zgoda, upoważnienie, oświadczenie) oraz klauzul informacyjnych stanowiących załączniki do niniejszej Polityki (załączniki od 1 do 8 oraz 12 i 13).

§ 9

REALIZACJA PRAW PRZEZ OSOBY, KTÓRYCH DANE DOTYCZĄ

1. W przypadku otrzymania żądania w postaci pisemnego wniosku dotyczącego prawa dostępu przysługującego osobie, której dane dotyczą należy:
   a) wniosek należy przekazać do IDO,
   b) IOD przygotowuje projekt odpowiedzi na wniosek,
   c) odpowiedź na żądanie podpisuje Administrator lub osoba przez niego upoważniona,
   d) odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencje można wysłać również drogą elektroniczną,
   e) IDO prowadzi rejestr wpływających wniosków.
2. W przypadku otrzymania żądania w postaci pisemnego wniosku dotyczącego prawa do sprostowania danych należy:
   f) wniosek należy przekazać do IDO,
   g) IOD zwraca się do ASI z prośbą o sprostowanie danych,
   h) ASI jest zobowiązany do sprostowania danych, o które wnioskował IOD w ciągu 10 dni,
   i) IOD przygotowuje projekt odpowiedzi na wniosek,
   j) odpowiedź na żądanie podpisuje Administrator lub osoba przez niego

upoważniona,

k) odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencje można wysłać również drogą elektroniczną,

l) IDO prowadzi rejestr wpływających wniosków.

3. W przypadku otrzymania żądania w postaci pisemnego wniosku dotyczącego prawa do:
   1) usunięcia danych („prawo do bycia zapomnianym”),
   2) ograniczenia przetwarzania,
   3) przenoszenia danych,
   4) sprzeciwu,

   należy:
   5) wniosek należy przekazać do IDO,
   6) IOD ocenia zasadność wniosku:
   7) w przypadku, gdy żądanie nie jest zasadne:
      a) IOD przygotowuje odpowiedź do akceptacji i podpisu Administratora lub osoby upoważnionej,
      b) odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencje można wysłać również drogą elektroniczną,
   8) w przypadku, gdy żądanie jest zasadne:
      a) IOD zwraca się do ASI z prośbą o realizację żądań zawartych we wniosku,
      b) ASI jest zobowiązany do realizacji wniosku IOD w ciągu 10 dni,
      c) IOD przygotowuje projekt odpowiedzi na wniosek,
      d) odpowiedź na wniosek podpisuje Administrator lub osoba upoważniona,
      e) odpowiedź przekazywana jest adresatowi w formie listu poleconego za potwierdzeniem odbioru, jeżeli żądanie przyszło drogą elektroniczną i istnieje możliwość weryfikacji nadawcy, korespondencje można wysłać również drogą elektroniczną,

9) IOD prowadzi rejestr wniosków.

2. ADM udziela odpowiedzi na żądania osób, których dane dotyczą, bez zbędnej zwłoki, najpóźniej w terminie miesiąca, a jeżeli nie zamierza spełnić takiego żądania zobowiązany jest do podania przyczyny. Jeżeli żądanie ma skomplikowany charakter podmiot danych skierował dużą liczbę żądań, ADM czas udzielenia odpowiedzi może wydłużyć o kolejne dwa miesiące**,** jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi.

3. W przypadku jakichkolwiek zmian w zbiorach danych wynikających z realizacji praw osób, których dane dotyczą, ADM zobowiązany jest poinformować bez zbędnej zwłoki odbiorców, którym je udostępnił (przekazanie do wiadomości odpowiedzi kierowanej do adresata).

§ 10

Dane osobowe mogą być udostępniane w następujących przypadkach:

1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych na podstawie przepisów prawa,
2) na podstawie umowy powierzenia zawartej z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych osobowych.

2. Dane osobowe udostępnia się na pisemny umotywowany wniosek, chyba że istnieją przepisy stanowiące inaczej.
3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH, NIEZBĘDNNYCH DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§11.

1. Wszelkie dokumenty zwierające dane osobowe przechowywane są w szafach i pomieszczeniach zamykanych na klucz.
2. Osoba będąca dysponentem kluczy jest zobowiązana nie przekazywać kluczy do budynków i pomieszczeń, w których przetwarzane są dane, osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
3. Osoba która utraciła posiadane klucze do pomieszczeń Administratora, w których przetwarzane są dane, niezwłocznie zgłasza tę okoliczność IDO i Administratorowi.
4. IDO i Administrator podejmują wszelkie niezbędne środki techniczne organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.

ŚRODKI BEZPIECZEŃSTWA STOSOWANE PODCZAS PRACY Z DANYMI

§ 12.

1. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.
2. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.
3. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie.
4. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania.
5. Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej.

POSTĘPOWANIE W RAZIE ZAISTNIENIA ZAGROŻENIA DLA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH LUB NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH

§ 13.

1. Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.
2. Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
   a) nieautoryzowany dostęp do danych,
   b) nieautoryzowane modyfikacje lub zniszczenie danych,
   c) udostępnienie danych nieautoryzowanym podmiotom,
   d) nielegalne ujawnienie danych,
   e) pozyskiwanie danych z nielegalnych źródeł.
3. Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych lub podejrzewa, że taka sytuacja miała miejsce, ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.
4. W przypadku podejrzenia lub stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora Ochrony Danych lub innej osób upoważnionych przez Administratora.
5. Wobec osoby, która naruszyła zasady ochrony danych osobowych lub w przypadku stwierdzonego naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby, zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne, porządkowe lub karne. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby dokonującej naruszenia lub uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
6. W przypadku podejrzenia lub stwierdzenia naruszenia zasad bezpieczeństwa danych osobowych lub naruszenia zabezpieczeń stosowanych przez Administratora dla ochrony przetwarzanych danych osobowych należy niezwłocznie zawiadomić IDO i Administratora.
7. W przypadku opisanym w ust. 1 przeprowadza się sprawdzenie doraźne. Sprawdzenie jest dokonywane niezwłocznie.
8. Przy dokonywaniu sprawdzenia IDO oraz osobom wyznaczonym do współpracy z nim przez Administratora przysługują uprawnienia wskazane w rozporządzeniu ministra

administracji i cyfryzacji w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych, w szczególności prawo do:

a) utrwalenia danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania na informatycznym nośniku danych lub dokonania wydruku tych danych;
b) odebrania wyjaśnień osoby, której czynności objęto sprawdzeniem;
c) sporządzeniu kopii otrzymanego dokumentu;
d) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych.

9. Inspektor Ochrony Danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając Raport według wzoru (Załącznik nr 9).
10. Inspektor Ochrony Danych zasięga potrzebnych mu opinii i proponuje działania naprawcze, w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych oraz terminu wznowienia przetwarzania danych osobowych i prowadzi Wykaz naruszeń według wzoru (Załącznik nr 10).
11. Jeżeli IDO jest długotrwale nieobecny Administrator w przypadku, o którym mowa w ust. 1 obowiązany jest przeprowadzić postępowanie wyjaśniające i ustalające skutki oraz przyczyny naruszenia lub narażenia na naruszenie zasad bezpieczeństwa i sposobów zabezpieczenia, w sposób odpowiadający czynnościom podejmowanym przez IDO w przypadku sprawdzenia doraźnego.

§ 14

POSTĘPOWANIE W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. IDO podejmuje decyzje o wprowadzeniu zmian w środkach zabezpieczeń fizycznych oraz w systemie organizacji pracy, stosownie do mogących ponownie wystąpić naruszeń bezpieczeństwa danych osobowych.
2. ASI podejmuje decyzje odnośnie zmian w sposobie zabezpieczenia systemu informatycznego.
3. Administrator podejmuje decyzje o wyciągnięciu konsekwencji wobec osoby odpowiedzialnej za naruszenie zasad bezpieczeństwa.
4. IDO przekazuje do PUODO w terminie do 72 godzin, zgłoszenie zawierające informacje o stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych:

1) w przypadku przekroczenia 72 godzinnego terminu dodatkowo do zgłoszenia dołącza wyjaśnienia,
2) w przypadku gdy informacji nie może udzielić w tym samym czasie, udziela ją sukcesywnie bez zbędnej zwłoki.

5. IDO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
6. Poinformowanie bez zbędnej zwłoki osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej sobie podjęcie niezbędnych działań zapobiegawczych. Należy przekazywać informację osobom, których dane dotyczą, tak

szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z PUODO, z poszanowaniem wskazówek przekazanych przez PUODO lub inne odpowiednie organy, takie jak organy ścigania. Zawiadomienie powinno przekazywać informację w jasnym i prostym języku a zawierać:

1) opis charakteru naruszenia ochrony danych osobowych,
2) zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków.

7. Poinformowanie, o którym mowa w pkt. 6 nie jest wymagane jeśli PUODO stwierdzi, że spełniony został jeden z poniższych warunków:
    1) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
    2) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
    3) 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.

PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRWANIEŃ W SYSTEMIE INFORMATYCZNYM

§ 15.

Użytkownikowi systemu informatycznego zostaje nadany dostęp na podstawie „Karty dostępu (zmiany) do przetwarzania danych w systemie informatycznym”, stanowiącej załącznik nr 11 do niniejszej Polityki, po uprzednim:

1. Zapoznaniu z przepisami dotyczącymi ochrony danych osobowych.
2. Podpisaniu oświadczenia o zapoznaniu się z niniejszą dokumentacją przetwarzania danych osobowych.
3. Podpisaniu oświadczenia o zachowaniu informacji (w tym danych osobowych), do których użytkownik będzie miał dostęp podczas wykonywania obowiązków służbowych lub zobowiązań umownych oraz środków ich zabezpieczania w tajemnicy (również po ustaniu łączącej strony umowy), w tym powstrzymanie się od wykorzystywania ich w celach pozasłużbowych.
4. Otrzymaniu upoważnienia do przetwarzania danych osobowych.

POLITYKA HASEŁ

§ 16.

1. Każdy użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.
2. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.

3. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez Administratora Systemu Informatycznego) i jego przechowywanie.
4. Każdy użytkownik posiadający dostęp do systemów informatycznego Administratora jest obowiązany do:
   1) zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
   2) niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
   3) niezwłocznej zmiany hasła tymczasowego, przekazanego przez Administratora Systemu Informatycznego;
   4) poinformowania Administratora Systemu Informatycznego oraz Inspektora Danych Osobowych o podejrzeniu lub rzeczywistym ujawnieniu hasła;
   5) stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych;
   6) stosowania haseł nie posiadających w swojej strukturze części loginu;
   7) stosowania haseł nie będących zbliżone do poprzednich (np.Tomasz$2013 - Tomasz$2014);
   8) zmiany wykorzystywanych haseł nie rzadziej niż raz na 30 dni.
5. Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
6. Zabronione jest:
   1) zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;
   2) stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
   3) używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
   4) udostępnianie haseł innym użytkownikom;
   5) przeprowadzanie prób łamania haseł;
   6) wpisywanie haseł „na stałe” (np. w skryptach logowania) oraz wykorzystywania opcji autozapamiętywania haseł (np. w przeglądarkach internetowych);
   7) po trzykrotnym, błędnym wprowadzeniu hasła użytkownik jest zobowiązany zgłosić ten fakt do Administratora Systemu Informatycznego, w celu zresetowania hasła dostępowego.

ZASADY POSTĘPOWANIA Z KLUCZAMI KRYPTOGRAFICZNYMI

§ 17.

1. W systemach obsługujących transmisję danych osobowych wrażliwych lub informacji poufnych Administratora powinny być wykorzystywane klucze kryptograficzne służące do zabezpieczenia danych.
2. Przekazywanie kluczy użytkownikom powinno odbywać się w sposób protokolarny, o ile nie następuje w drodze teletransmisji.
3. Obowiązkiem użytkownika jest zabezpieczenie kluczy (prywatnych) przed dostępem osób nieupoważnionych.

4. W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia o jego ujawnienie należy bezzwłocznie powiadomić Administratora Systemu Informatycznego oraz Inspektora Danych Osobowych.
5. Dane osobowe wrażliwe lub informacje poufne Administratora, do których nie stosuje się kluczy kryptograficznych, można przesyłać wyłącznie pocztą elektroniczną po uaktywnieniu funkcji podpisywania i szyfrowania pliku.
6. Każdy użytkownik korzystający z kluczy kryptograficznych jest zobowiązany do ich użytkowania i przechowywania w sposób uniemożliwiający utratę lub dostęp osób niepowołanych.
7. W przypadku podejrzenia lub rzeczywistego naruszenia bezpieczeństwa klucza fakt ten należy niezwłocznie zgłosić Administratorowi Systemu Informatycznego oraz Inspektorowi Ochrony Danych.

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE INFORMATYCZNYM

§ 18.

1. Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.
2. Zawieszenie pracy w systemie informatycznym tj. brak wykonywania jakichkolwiek czynności przez okres 5 minut w systemie informatycznym powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem. Zastosowanie powyższego mechanizmu nie zwalnia użytkownika z obowiązku każdorazowego blokowania ekranu wygaszaczem chronionym hasłem po odejściu od stanowiska.
3. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.
4. Przed zakończeniem pracy należy upewnić się czy dane zostały zapisane, aby uniknąć ich utraty danych.
5. Po zakończeniu pracy, użytkownik obowiązany jest wylogować się z systemu informatycznego przetwarzającego dane osobowe i z systemu operacyjnego, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.
6. Użytkownik systemu informatycznego przetwarzającego dane osobowe niezwłocznie powiadamia administratora systemu w przypadku, gdy:
   1) Wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;
   2) Niektóre opcje, dostępne użytkownikowi w normalnej sytuacji, przestały być dostępne lub też opcje niedostępne użytkownikowi w normalnej sytuacji, stały się dostępne.

ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ

§ 19.

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie Administratora.

2. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej Administratora w postaci książki adresowej.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Administratora podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci Administratora (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
4. Wszelka korespondencja elektroniczna prowadzona przez pracownika, a niezwiązana z działalnością Administratora, powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.
5. Użytkownicy mają prawo korzystać z systemu poczty elektronicznej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
6. Korzystanie z systemu 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 lub umownych, a także na wydajność systemu poczty elektronicznej.
7. Zabronione jest:
   1) wysyłanie bez zgody Administratora materiałów służbowych zawierających chronione dane na konta prywatne (np. celem pracy nad dokumentami poza miejscem pracy);
   2) wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Administratora;
   3) odbieranie przesyłek z nieznanych źródeł;
   4) otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
   5) przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych oraz plików graficznych bez zgody Administratora;
   6) ukrywanie lub dokonywanie zmian tożsamości nadawcy;
   7) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;
   8) odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją administratorowi systemu informatycznego;
   9) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
   10) wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Administratora lub do poszukiwania dodatkowego zatrudnienia.

ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET)

§ 20.

1. Zdalne korzystanie z systemów informatycznych poprzez sieć publiczną może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.

2. Zdalny dostęp do serwerów w celach administracyjnych może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
3. Dostęp użytkowników do sieci publiczne (Internet) powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy.
4. Wprowadza się całkowity zakaz w dostępie do treści niezgodnych z prawem lub niestosownych, a w szczególności pornograficznych, rasistowskich, traktujących o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.

ZASADY POSTĘPOWANIA Z NOŚNIKAMI ELEKTRONICZNYMI ORAZ VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH

§ 21.

1. Każdy użytkownik wymiennych nośników elektronicznych oraz użytkownicy zdalnych dostępów do sieci służbowej Administratora (VPN) oraz użytkownicy elektronicznych kart dostępu ponoszą całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz są obowiązani do stosowania się do poniższych zasad:
   1) Zabrania się pozostawiania bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje Administratora;
   2) Komputery przenośne należy przewozić jako bagaż podręczny i w miarę możliwości maskować je;
   3) Użytkownik wykonując czynności zawodowe lub umowne poza stałym miejscem wykonywania obowiązków powinien zadbać o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich;
   4) Zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem;
   5) Zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością SP w Romanowie Dolnym ;
   6) W przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do bezpośredniego przełożonego lub administratora systemu informatycznego. Bezpośredni przełożony lub administrator systemu informatycznego bezzwłocznie zgłaszają taki fakt do Inspektora Danych Osobowych, ponieważ zagubienie nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez Administratora;
   7) Problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać administratorowi systemu informatycznego.

UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH

§ 22.

1. Do sprzętu komputerowego zalicza się między innymi:
   1) komputery stacjonarne,
   2) komputery przenośne,
   3) tablety,
   4) smartphony,

5) drukarki,
6) modemy,
7) monitory,
8) routery,
9) osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe.

2. Administrator udziela pomocy użytkownikowi w obsłudze sprzętu i oprogramowania.
3. W przypadku niepoprawnego i niezgodnego z przeznaczeniem użytkowania przez użytkownika sprzętu komputerowego, administrator systemu informatycznego informuje o powyższym Inspektora Danych Osobowych.
4. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
5. Użytkownik nie może samodzielnie zmieniać konfiguracji przekazanego sprzętu komputerowego oraz instalować, usuwać oprogramowania, w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania.

KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ, FAKSOWEJ I WIZYJNEJ

§ 23.

1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji danych osobowych lub informacji poufnych Administratora, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
2. Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
3. Zabronione jest wykorzystywanie domyślnych („fabrycznych") haseł dla ww. urządzeń.
4. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających dane osobowe wrażliwe lub informacje poufne Administratora jest zabronione.
5. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających informacje wrażliwe.

OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM

§ 24.

1. Zidentyfikowanymi obszarami systemu informatycznego Administratora narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, pamięć RAM oraz elektroniczne nośniki informacji.
2. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.
3. Użytkownicy systemu mają obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.

4. W przypadku stwierdzenia pojawienia się wirusa i braku możliwości usunięcia go przez program antywirusowy, użytkownik powinien skontaktować się z administratorem systemu informatycznego.

POSTANOWIENIA KOŃCOWE

§ 25.

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Polityki potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
2. W sprawach nieuregulowanych w Polityce ochrony danych osobowych mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz 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).
3. Polityka jest dostępna w siedzibie Administratora.

Załączniki:

1) ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH
2) UPOWAŻNEINIE DO PRZETWARZANIA DANYCH OSOBOWYCH OŚWIADCZENIE PRACOWNIKA
3) UPOWAŻNIENIE NR do przebywania w obszarze przetwarzania danych osobowych OŚWIADCZENIE PRACOWNIKA
4) ODWOŁANIE UPOWAŻNIENIE NR ……
5) INFORMACJA W SEKRETARIACIE i NA STRONIE INTERNETOWEJ
6) KANDYDACI DO PRACY
7) ZATRUDNIENI
8) ZAMÓWIENIA PUBLICZNE i ZAOPATRZENIE
9) RAPORT
10) WYKAZ INCYDENTÓW
11) WZÓR KARTY
12) ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH WYCHOWANKA SZKOŁY W ZWIĄZKU Z PROCESEM EDUKACJI
13) ZGODA NA PRZETWARZANIE WIZERUNKU

Załącznik nr 1

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH DZIECKA

Ja, niżej podpisana/y ……., **legitymujący się dowodem osobistym/paszportem/kartą pobytu serii** …… **o numerze** ……..……**,** jako opiekun

……

(imię i nazwisko dziecka), **wyrażam zgodę na*:**

- ○ przetwarzanie danych osobowych mojego dziecka przez Szkołę Podstawową w Romanowie Dolnym, Romanowo Dolne 124, 64-700 Czarnków, do celów realizacji zadań ustawowych i statutowych,
- ○ przetwarzanie danych osobowych mojego dziecka przez Szkołę Podstawową w Romanowie Dolnym, Romanowo Dolne 124, 64-700 Czarnków, do celów promocyjnych,
- ○ przetwarzanie danych osobowych mojego dziecka przez Szkołę Podstawową w Romanowie Dolnym, Romanowo Dolne 124, 64-700 Czarnków, w związku ze zautomatyzowanym podejmowaniem decyzji w indywidualnych sprawach, w tym przekazywaniem danych osobowych do państwa trzeciego.

Szkoła Podstawowa w Romanowie Dolnym, Romanowo Dolne 124, 64-700 Czarnków, przetwarza dane osobowe na następującym/ch **portalu/ach społecznościowym/ch: …….,** co oznacza **automatyczne przetwarzanie danych** oraz ich profilowanie przez właściciela portalu oraz przekazywanie danych osobowych tj. np. wizerunek - udostępnionych na tym portalu/ach - do Państw Trzecich (poza obszar UE).

proszę zaznaczyć zakres zgody

Rozumiem, że dane osobowe mojego dziecka mogą być przetwarzane z pominięciem mojej zgody w następujących sytuacjach:

a) przetwarzanie jest niezbędne do wykonania umowy lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
b) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
d) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
e) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem

sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Zgodnie z art. 4 ust. pkt. 7 RODO **Administratorem** danych osobowych Pani/Pana dziecka jest **Szkoła Podstawowa w Romanowie Dolnym, Romanowo Dolne 124, 64-700 Czarnków,** reprezentowana przez **Dyrektora SP W ROMANOWIE DOLNYM - Kierownika Jednostki.**

Podanie danych osobowych jest dobrowolne lub wynika z obowiązku podania danych na podstawie przepisów obowiązującego prawa lub przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania. Dokumenty zawierające dane osobowe Pani/Pana dziecka będą przetwarzane przez okres określony przepisami prawa. Przetwarzane dane osobowe mogą być udostępniane innym podmiotom zwłaszcza, gdy obowiązek taki wynika z powszechnie obowiązujących przepisów prawa lub na podstawie niniejszej - wyrażonej przez Panią/Pana - zgody.

Ma Pani/Pan prawo wycofać zgodę w każdym momencie, w formie ustnej lub pisemnej.

……..…….……

Data, miejsce i podpis osoby wyrażającej zgodę*

Załącznik Nr 2

UPOWAŻNIENIE NR ……..

do przetwarzania danych osobowych

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady Europy (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) oraz ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Poz. 1000) upoważniam:

Panią/Pana: …….

wykonującą/wykonującego obowiązki ……
w Szkole Podstawowej w Romanowie Dolnym, Romanowo Dolne 124, 64-700 Czarnków,

……

(pieczęć instytucji)

do przetwarzania danych osobowych, w celach związanych z wykonywaniem zadań wynikających z zakresu obowiązków i czynności w systemach kartotekowych oraz informatycznych* (dostęp do modułów oraz danych zgodnie z prawem dostępu nadanym przez administratora), w kategoriach:

- danych osobowych uczniów i nauczycieli z podzbiorami w zakresie: wprowadzanie, wgląd, modyfikacja, dodawanie, usuwanie, drukowanie*
- danych pracowniczych z podzbiorami w zakresie: wprowadzanie, wgląd, modyfikacja, dodawanie, usuwanie, drukowanie*
- danych administracyjnych z podzbiorami w zakresie: wprowadzanie, wgląd, modyfikacja, dodawanie, usuwanie, drukowanie*
- danych doraźnych w zakresie: wprowadzanie, wgląd, modyfikacja, dodawanie, usuwanie, drukowanie*

w okresie: na czas stażu/praktyki/ zatrudnienia/ wolontariatu *

……

Pieczęć i podpis Administratora Danych lub upoważnionego przedstawiciela

……., dnia …….....

***niepotrzebne skreślić**

OŚWIADCZENIE PRACOWNIKA

Ja niżej podpisany/na oświadczam, iż zostałem/zostałam* przeszkolony/przeszkolona* w zakresie ochrony danych osobowych i znana jest mi treść **Polityki Ochrony Danych Osobowych** wraz z załącznikami i zobowiązuję się:

- do przestrzegania i stosowania zasad zawartych w wyżej wymienionych dokumentach,
- zachować w tajemnicy dane w tym dane osobowe, z którymi zetknąłem/zetknęłam* się w trakcie wykonywania swoich zadań, zarówno w czasie trwania umowy jak i po jej zakończeniu,
- chronić dane w tym dane osobowe przed dostępem osób nieupoważnionych, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem polityki bezpieczeństwa i ustawy oraz zmianą, utratą, ujawnieniem, uszkodzeniem lub zniszczeniem.

……

Czytelny podpis pracownika

……

Podpis Inspektora Ochrony Danych

* niewłaściwe skreślić lub wpisać właściwe

Załącznik nr 3

UPOWAŻNIENIE NR ……..
do przebywania w obszarze przetwarzania danych osobowych

WAŻNOŚĆ:

Od* .....
Do* .....
Na czas trwania stosunku pracy*

UPOWAŻNIENIE
DO PRZEBYWANIA W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie pkt 1.2 załącznika do Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., NR 100, poz. 1024 ze zm.) UPOWAŻNIAM Panią/Pana*:

.....
(imię i nazwisko pracownika)

……
(stanowisko)

do przebywania w pomieszczeniach, w których przetwarzane są dane osobowe, w czasie niezbędnym do wykonywania obowiązków służbowych.

.....
Podpis Kierownika Jednostki

* niewłaściwe skreślić lub wpisać właściwe

OŚWIADCZENIE PRACOWNIKA

Ja niżej podpisany/na oświadczam, iż zostałem/zostałam* przeszkolony/przeszkolona* w zakresie ochrony danych osobowych i znana jest mi treść **Polityki Ochrony Danych Osobowych** wraz z załącznikami i zobowiązuję się:

- do przestrzegania i stosowania zasad zawartych w wyżej wymienionych dokumentach,
- zachować w tajemnicy dane w tym dane osobowe, z którymi zetknąłem/zetknęłam* się w trakcie wykonywania swoich zadań, zarówno w czasie trwania umowy jak i po jej zakończeniu,
- chronić dane w tym dane osobowe przed dostępem osób nieupoważnionych, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem polityki bezpieczeństwa i ustawy oraz zmianą, utratą, ujawnieniem, uszkodzeniem lub zniszczeniem.

……

Czytelny podpis pracownika

……

Podpis Inspektora Ochrony Danych

* niewłaściwe skreślić lub wpisać właściwe

Załącznik nr 4

ODWOŁANIE UPOWAŻNIENIE NR ……..

ODWOŁANIE UPOWAŻNIENIA

do przetwarzania danych osobowych

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady Europy (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 (RODO), odwołuję z dniem …….. upoważnienie nr …… z dnia …….. do przetwarzania danych osobowych wydane Pani/Panu*:

.....

(imię i nazwisko pracownika)

……

(stanowisko)

……..

……

Podpis sporządzającego *Podpis Kierownika Jednostki*

* niewłaściwe skreślić lub wpisać właściwe

Załącznik nr 5

Informacja w Sekretariacie i na stronie internetowej

Klauzula informacyjna

Klauzula informacyjna dot. przetwarzania danych osobowych na podstawie obowiązku prawnego ciążącego na administratorze (przetwarzanie w związku z ustawą Prawo Oświatowe)	
TOŻSAMOŚĆ ADMINISTRATORA I WSPÓŁ-ADMINISTRATORÓW	Administratorem Danych Osobowych jest: **Dyrektor Szkoły Podstawowej w Romanowie Dolnym,** Romanowo Dolne 124, 64-700 Czarnków, w zakresie rejestracji oraz przetwarzania danych i przechowywanej dokumentacji pisemnej; a współadministratorami: 1. **Dyrektor Gminnego Zespołu Obsługi Oświaty (GZOO) w Czarnkowie** z siedzibą przy ul. Rybaki 3, 64-700 Czarnków, w zakresie rejestracji oraz przetwarzania danych i przechowywanej dokumentacji pisemnej; 2. **Wójt Gminy Czarnków** z siedzibą Urzędu Gminy przy ul. Rybaki 3, 64-700 Czarnków,, w zakresie rejestracji oraz przetwarzania danych i przechowywanej dokumentacji pisemnej, 3. **Wielkopolski Kurator Oświaty w Poznaniu** z siedzibą przy ul. Kościuszki 93, 61-716 Poznań, w zakresie rejestracji oraz przetwarzania danych i przechowywanej dokumentacji pisemnej.
DANE KONTAKTOWE ADMINISTRATORA, WSPÓŁ-ADMINISTRATORÓW I DANE KONTAKTOWE INSPEKTORA OCHRONY DANYCH	Z administratorem – **Dyrektorem Szkoły Podstawowej w Romanowie Dolnym,** Romanowo Dolne 124, 64-700 Czarnków, można się skontaktować pisemnie na adres siedziby administratora lub z wyznaczonym przez niego inspektorem ochrony danych osobowych pod adresem: kontakt@smart-standards.com albo pod numerem tel. +48 602 24 12 39, a z pozostałymi: 1. Z współadministratorem – **Dyrektorem Gminnego Zespołu Obsługi Oświaty (GZOO) w Czarnkowie** można się skontaktować pisemnie na adres siedziby administratora lub z wyznaczonym przez niego inspektorem ochrony danych osobowych pod adresem: kontakt@smart-standards.com albo pod numerem tel. +48 602 24 12 39 2. Z współadministratorem – **Wójtem Gminy Czarnków** można się skontaktować pisemnie na adres siedziby administratora lub z wyznaczonym przez niego inspektorem ochrony danych osobowych pod adresem: kontakt@smart-standards.com albo pod numerem tel. +48 602 24 12 39 3. Z współadministratorem – **Wielkopolskim Kuratorem Oświaty** można się skontaktować pisemnie na adres siedziby administratora lub z wyznaczonym przez niego

	inspektorem ochrony danych osobowych pod adresem: ido@ko-poznan.pl, tel. +48 780 386 035 Z każdym z wymienionych inspektorów ochrony danych można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych, które pozostają w jego zakresie działania.
CELE PRZETWARZANIA I PODSTAWA PRAWNA	Pani / Pana dane oraz dane Pani/Pana dziecka/podopiecznego będą przetwarzane na podstawie art. 6 ust. 1 lit. c w związku z art. 13 ust. 1 i 2 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) (Dz. Urz. UE L 119 z 04.05.2016, z późn. zm.) (dalej: RODO) w związku z przepisami ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe (t.j. Dz. U. z 2019 r. poz. 1148 i 1078) oraz rozporządzenia Ministra Edukacji Narodowej z dnia 16 marca 2017 r. w sprawie przeprowadzania postępowania rekrutacyjnego oraz postępowania uzupełniającego do publicznych przedszkoli, szkół i placówek (Dz.U. 2017 poz. 610) w celach weryfikacji danych o miejscu spełnienia obowiązku przedszkolnego, szkolnego lub nauki w roku szkolnym 2019/2020 oraz wykonania ciążących na Administratorze obowiązków prawnych wynikających z przepisów Prawa oświatowego.
ODBIORCY DANYCH	Odbiorcami danych są podmioty przetwarzające te dane. Pani/Pana dane osobowe oraz dane osobowe Pani/Pana dziecka/podopiecznego mogą być udostępnione podmiotom: • służbom; organom administracji publicznej; sądom i prokuraturze; komornikom sądowym; państwowym i samorządowym jednostkom organizacyjnym oraz innym podmiotom – w zakresie niezbędnym do realizacji zadań publicznych; • osobom i jednostkom organizacyjnym, jeżeli wykażą w tym interes prawny; • osobom i jednostkom organizacyjnym, jeżeli wykażą w tym interes faktyczny w otrzymaniu danych, pod warunkiem uzyskania zgody Pani /Pana zgody; • jednostkom organizacyjnym, w celach badawczych, statystycznych, badania opinii publicznej, jeżeli po wykorzystaniu dane te zostaną poddane takiej modyfikacji, która nie pozwoli ustalić tożsamości osób, których dane dotyczą; przez: • Dyrektora Szkoły Podstawowej w Romanowie Dolnym - podmiotom uprawnionym w trybie indywidualnych zapytań;

	• Dyrektora GZOO w Czarnkowie - podmiotom uprawnionym w trybie indywidualnych zapytań; • Wójta Gminy Czarnków - podmiotom uprawnionym w trybie indywidualnych zapytań, • Wielkopolskiego Kuratora Oświaty - podmiotom uprawnionym w trybie indywidualnych zapytań. Pani/Pana dane oraz dane Pani/Pana dziecka lub podopiecznego mogą być udostępnione stronom postępowań administracyjnych prowadzonych na podstawie Kodeksu postępowania administracyjnego, których jest Pan/Pani i/lub Pana/Pani podopieczny stroną/stronami lub uczestnikiem/uczestnikami w trybie udostępnienia akt tych postępowań.
OKRES PRZECHOWYWANIA DANYCH	Dane zgromadzone w formie pisemnej są przetwarzane zgodnie z klasyfikacją wynikająca z jednolitego rzeczowego wykazu akt organów gminy i związków międzygminnych oraz urzędów obsługujących te organy i związki na podstawie przepisów rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011r. Dz.U. Nr 14, poz. 67), tj. 10 lat.
PRAWA PODMIOTÓW DANYCH	Przysługuje Pani/Panu prawo dostępu do Pani/Pana danych oraz prawo żądania ich sprostowania.
PRAWO WNIESIENIA SKARGI DO ORGANU NADZORCZEGO	Przysługuje Pani/Panu również prawo wniesienia skargi do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych Biuro Prezesa Urzędu Ochrony Danych Osobowych Adres: Stawki 2, 00-193 Warszawa Telefon: 22 531 03 00
INFORMACJA O DOWOLNOŚCI LUB OBOWIĄZKU PODANIA DANYCH	Obowiązek podania danych osobowych wynika z przepisów prawa, w szczególności rozporządzenia Ministra Edukacji Narodowej z dnia 16 marca 2017 r. w sprawie przeprowadzania postępowania rekrutacyjnego oraz uzupełniającego do publicznych przedszkoli, szkół i placówek oświatowych (Dz.U. 2017 poz. 610).

UWAGA: Szkoła Podstawowa w Romanowie Dolnym, Romanowo Dolne 124, 64-700 Czarnków, nie przetwarza / przetwarza dane* osobowe na następującym/ch **portalu/ach społecznościowym/ch:**

……..,

co oznacza **automatyczne przetwarzanie danych** oraz ich profilowanie przez właściciela portalu oraz przekazywanie danych osobowych tj. np. wizerunek - udostępnionych na tym portalu/ach - do Państw Trzecich (poza obszar UE).

* niewłaściwe skreślić lub wpisać właściwe

Załącznik nr 6

Klauzula informacyjna KANDYDACI DO PRACY

1. **Administratorem Pani/Pana danych osobowych jest Szkoła Podstawowa w Romanowie Dolnym, Romanowo Dolne 124, 64-700 Czarnków, reprezentowana przez Dyrektora Szkoły.**
2. **Cele i podstawy prawne przetwarzania Pana / Pani danych osobowych to:**

a) art. 6 ust 1 lit. a i b RODO tj. rekrutacja,
b) art. 6 ust. 1 lit. c RODO tj. pozyskiwanie informacji o niekaralności zgodnie z ustawą z dnia 12 kwietnia 2018 r. o zasadach pozyskiwania informacji o niekaralności osób ubiegających się o zatrudnienie i osób zatrudnionych na podst. ustawy z dnia 12 kwietnia 2018 r. o zasadach pozyskiwania informacji o niekaralności osób ubiegających się o zatrudnienie i osób zatrudnionych w podmiotach sektora finansowego,
c) art. 9 ust. 2 lit. b RODO tj. w zakresie w jakim przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez pracodawcę w dziedzinie prawa pracy, w tym przetwarzania danych do oceny zdolności pracownika do pracy.

3. **Pani/Pana dane osobowe mogą być przekazywane następującym odbiorcom danych:**

a) bankom - celem wypłaty wynagrodzeń,
b) organom państwowym (np. ZUS, US i innym uprawnionym na podstawie przepisów prawa) - celem wykonania ciążących na Administratorze obowiązków,
c) podmiotom świadczącym benefity dla pracowników i współpracowników,
d) podmiotom świadczącym usługi grupowego ubezpieczenia pracowników i współpracowników,
e) podmiotom świadczącym usługi pocztowe tj. Poczta Polska i Kurierzy,
f) podmiotom obsługującym nasze systemy teleinformatyczne (hosting, dostawcom usług IT),
g) podmiotom świadczącym dla nas usługi z zakresu pomocy prawnej, kadrowej, audytu wewnętrznego, księgowości, podatków lub usługi doradcze.

4. **Czas przetwarzania danych to okres rekrutacji, realizacji umowy oraz czas po jej ustaniu:**

a) przez 1 rok od zakończenia procesu rekrutacji;
b) dane osobowe przetwarzane na podstawie prawnie uzasadnionego interesu Administratora do czasu wniesienia sprzeciwu przez osobę, której dane dotyczą jednak ni dłużej niż 10 lat.

5. **Administrator wyznaczył Inspektora Ochrony Danych** nadzorującego prawidłowość przetwarzania danych osobowych, z którym można się kontaktować pod numerem telefonu 602 241 239 (w godzinach 10:00-20:00) bądź wysyłając informację na adres e-mail: kontakt@smart-standards.com lub jmrowicka@poczta.onet.pl, tel.
6. **Podane dane będą przetwarzane na podstawie** art. 22` § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity: Dz.U. z 2018 r. , poz. 917) oraz Pani/Pana zgody na przetwarzanie danych osobowych.
7. Podanie danych w zakresie wynikającym z Kodeksu pracy jest obowiązkowe, pozostałe dane przetwarzamy za Pani/Pana zgodą na przetwarzanie.
8. **Dane nie będą udostępniane podmiotom zewnętrznym**, przekazywane do państwa trzeciego lub organizacji międzynarodowych oraz nie będą podlegały profilowaniu.
9. **Dane przechowywane będą przez okres:** wynikający z Kodeksu Pracy bądź do odwołania przez Panią/Pana zgody na przetwarzanie danych osobowych.

10. **Posiada Pani/Pan prawo dostępu do treści swoich danych** oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie.
11. **Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych osobowych, ul. Stawki 2, 00-193 Warszawa, Infolinia: 606 950 000 (w godzinach 10.00 – 13.00),** e-mail: kancelaria@giodo.gov.pl.

Wyrażam zgodę na przetwarzanie moich danych osobowych przez Szkołę Podstawową w Romanowie Dolnym, Romanowo Dolne 124, 64-700 Czarnków, reprezentowaną przez Dyrektora Szkoły 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 w celu przeprowadzenia procesu rekrutacji oraz towarzyszących mu czynności wymaganych przepisami prawa. Została/em poinformowany o moich prawach i obowiązkach. Przyjmuję do wiadomości, iż podanie przeze mnie danych osobowych jest dobrowolne.

....

(miejscowość i data) (czytelny podpis pracownika)

Załącznik nr 7

Klauzula informacyjna ZATRUDNIENI

1.Administratorem Pani/Pana danych osobowych jest Szkoła Podstawowa w Romanowie Dolnym, Romanowo Dolne 124, 64-700 Czarnków, reprezentowana przez Dyrektora Szkoły.

2. **Cele i podstawy prawne przetwarzania Pana / Pani danych osobowych to:**

d) art. 6 ust 1 lit. a i b RODO tj. zawarcie i realizacja umowy o pracę,

e) art. 6 ust 1 lit. c RODO wykonanie obowiązków wynikających z prawa pracy lub zawartej umowy cywilnoprawnej, przez co rozumiemy także wykonywanie obowiązków z zakresu BHP, rozliczanie wszelkich należności, zgłaszanie pracowników do odpowiednich urzędów czy archiwizowania akt osobowych,

f) art. 6 ust. 1 lit. c RODO tj. pozyskiwanie informacji o niekaralności zgodnie z ustawą z dnia 12 kwietnia 2018 r. o zasadach pozyskiwania informacji o niekaralności osób ubiegających się o zatrudnienie i osób zatrudnionych na podst. ustawy z dnia 12 kwietnia 2018 r. o zasadach pozyskiwania informacji o niekaralności osób ubiegających się o zatrudnienie i osób zatrudnionych w podmiotach sektora finansowego,

g) art. 6 ust. 1 lit. c RODO tj. wypełnienie obowiązku prawnego wynikającego z art. 8 ustawy o zakładowym funduszu świadczeń socjalnych z dnia 9 listopada 2017 r. oraz z regulaminu ZFŚS,

h) art. 6 ust. 1 lit. f RODO tj. realizacja prawnie uzasadnionego interesu administratora tj. dochodzenia ewentualnych roszczeń związanych z zawartą umową o pracę, stosowanym monitoringiem wizyjnym/monitoringiem poczty e-mail/monitoringiem Internetu/ monitoringiem pojazdów służbowych,

i) art. 9 ust. 2 lit. b RODO tj. w zakresie w jakim przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez pracodawcę w dziedzinie prawa pracy, w tym przetwarzania danych do oceny zdolności pracownika do pracy.

3. **Pani/Pana dane osobowe mogą być przekazywane następującym odbiorcom danych:**

h) bankom - celem wypłaty wynagrodzeń,

i) organom państwowym (np. ZUS, US i innym uprawnionym na podstawie przepisów prawa) - celem wykonania ciążących na Administratorze obowiązków,

j) podmiotom świadczącym benefity dla pracowników i współpracowników,

k) podmiotom świadczącym usługi grupowego ubezpieczenia pracowników i współpracowników,

l) podmiotom świadczącym usługi pocztowe tj. Poczta Polska i Kurierzy,

m) podmiotom obsługującym nasze systemy teleinformatyczne (hosting, dostawcom usług IT),

n) podmiotom świadczącym dla nas usługi z zakresu pomocy prawnej, kadrowej, audytu wewnętrznego, księgowości, podatków lub usługi doradcze.

4. Czas przetwarzania danych to okres rekrutacji, realizacji umowy oraz czas po jej ustaniu:

c) do momentu przedawnienia roszczeń z tytułu umowy o pracę m.in. zgodnie z art. 291 Kodeksu Pracy tj. co do zasady przez okres 3 lat, a w zakresie umów cywilnoprawnych m.in. zgodnie z art. 118 Kodeksu Cywilnego tj. co do zasady przez okres 3 lat;

d) do momentu wygaśnięcia obowiązku ich archiwizacji tj. akta kadrowe archiwizowane są przez okres 50 lat od dnia zakończenia przez ubezpieczonego pracownika pracy bądź okres do 10 lat m.in. dla umów zawieranych po 1 stycznia 2019 r.;
e) dane osobowe zawarte w dokumentacji na podstawie, której przyznano świadczenia z ZFŚS oraz w pozostałej dokumentacji np. we wnioskach pracowników o świadczenia będą przechowywane przez okres 5 lat, z tym, że dokumenty płatnicze, które są dowodem opłacenia składek oraz terminu ich opłacenia będą przechowywane do czasu przedawnienia zobowiązań podatkowych;
f) dane osobowe przetwarzane na podstawie prawnie uzasadnionego interesu Administratora do czasu wniesienia sprzeciwu przez osobę, której dane dotyczą jednak ni dłużej niż 10 lat.

5. **Administrator wyznaczył Inspektora Ochrony Danych** nadzorującego prawidłowość przetwarzania danych osobowych, z którym można się kontaktować pod numerem telefonu 602 241 239 (w godzinach 10:00-20:00) bądź wysyłając informację na adres e-mail: kontakt@smart-standards.com lub jmrowicka@poczta.onet.pl
6. **Podane dane będą przetwarzane na podstawie** art. 22` § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jednolity: Dz.U. z 2018 r. , poz. 917) oraz Pani/Pana zgody na przetwarzanie danych osobowych.
7. Podanie danych w zakresie wynikającym z Kodeksu pracy jest obowiązkowe, pozostałe dane przetwarzamy za Pani/Pana zgodą na przetwarzanie.
8. **Dane nie będą udostępniane podmiotom zewnętrznym**, przekazywane do państwa trzeciego lub organizacji międzynarodowych oraz nie będą podlegały profilowaniu.
9. **Dane przechowywane będą przez okres:** wynikający z Kodeksu Pracy bądź do odwołania przez Panią/Pana zgody na przetwarzanie danych osobowych.
10. **Posiada Pani/Pan prawo dostępu do treści swoich danych** oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie.
11. **Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych osobowych, ul. Stawki 2, 00-193 Warszawa, Infolinia: 606 950 000 (w godzinach 10.00 – 13.00),** e-mail: kancelaria@giodo.gov.pl.

Wyrażam zgodę na przetwarzanie moich danych osobowych przez Szkołę Podstawową w Romanowie Dolnym, Romanowo Dolne 124, 64-700 Czarnków, reprezentowaną przez Dyrektora Szkoły 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 w celu realizacji umowy o pracę oraz towarzyszących jej warunków zatrudnienia i ich zmiany. Została/em poinformowany o moich prawach i obowiązkach. Przyjmuję do wiadomości, iż podanie przeze mnie danych osobowych jest dobrowolne.

....

(miejscowość i data) (czytelny podpis pracownika)

Załącznik nr 8

Klauzula informacyjna ZAMÓWIENIA PUBLICZNE i ZAOPATRZENIE

1. **Szkoła Podstawowa w Romanowie Dolnym przy ulicy Romanowo Dolne 124, 64-700 Czarnków, jako Administrator danych osobowych reprezentowany przez Dyrektora Szkoły, przetwarza Pani/Pana dane osobowe w celu realizacji zadań ustawowych i statutowych, w tym** w sprawach objętych przedmiotem postępowania o udzielenie zamówienia publicznego oraz zawarcia umowy na zakup materiałów lub usług.
2. Dane osobowe przetwarzane są w celu prawidłowej realizacji umowy, przedstawienia ofert, świadczenia usług, ewidencji faktur za usługi, materiały, towary wykonane bądź zakupione, realizacji czynności finansowych, obsługi gwarancyjnej i pogwarancyjnej, obsługi reklamacji, obsługi promocji, obsługi programów partnerskich i wypełniania obowiązków wynikających z przepisów prawa.
3. Dane osobowe pozyskiwane są bezpośrednio od klientów, kontrahentów oraz potencjalnych klientów, jak i ze źródeł ogólnodostępnych.
4. Pani/Pana dane osobowe są przetwarzane w formie tradycyjnej oraz elektronicznej zgodnie z obowiązującymi przepisami prawa w tym Art. 6 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady Europy (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 (RODO), związanych z prowadzeniem postępowań o udzielenie zamówienia publicznego i wynikających z przepisów obowiązującego prawa, w tym ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 z późn. zm. oraz **przepisami odsyłającymi do tych ustaw**.
5. Zgodnie z Art. 4 pkt 7 RODO **Administratorem** Pani/Pana danych osobowych jest **Szkoła Podstawowa w Romanowie Dolnym, Romanowo Dolne 124, 64-700 Czarnków, reprezentowana przez Dyrektora Szkoły .**
6. Podanie danych osobowych jest dobrowolne lub wynika z obowiązku podania danych na podstawie przepisów obowiązującego prawa lub przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania.
7. Podanie przez Panią/Pana danych osobowych w zakresie niezbędnym do realizacji umów i kontraktów jest obowiązkowe, a w pozostałym zakresie jest dobrowolne. Konsekwencją niepodania niezbędnych danych osobowych może być rezygnacja z nawiązania z Państwem współpracy.
8. **Przetwarzane dane osobowe nie są i nie będą udostępniane innym podmiotom** poza przypadkami, gdy obowiązek taki wynika z powszechnie obowiązujących przepisów prawa lub zostanie na to wyrażona Pani/Pana zgoda. Dane nie będą przekazywane do państwa trzeciego ani organizacji międzynarodowej oraz nie będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania.
9. Dane osobowe będą przetwarzane na podstawie prawnie uzasadnionego interesu Administratora do czasu wniesienia sprzeciwu przez osobę, której dane dotyczą jednak nie dłużej niż 10 lat.
10. **Administrator wyznaczył Inspektora Ochrony Danych** nadzorującego prawidłowość przetwarzania danych osobowych, z którym można się kontaktować pod numerem telefonu 602 241 239 (w godzinach 10:00-20:00) bądź wysyłając informację na adres e-mail: kontakt@smart-standards.com lub jmrowicka@poczta.onet.pl
11. **Dane nie będą udostępniane podmiotom zewnętrznym**, przekazywane do państwa trzeciego lub organizacji międzynarodowych oraz nie będą podlegały profilowaniu.
12. **Posiada Pani/Pan prawo dostępu do treści swoich danych** oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie.
13. **Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych osobowych, ul. Stawki 2, 00-193 Warszawa, Infolinia: 606 950 000 (w godzinach 10.00 – 13.00),** e-mail: kancelaria@giodo.gov.pl.

Załącznik nr 9

WZÓR Raport

z naruszenia ochrony danych osobowych według wzoru PUODO

Załącznik nr 10

WYKAZ INCYDENTÓW POWODUJĄCYCH NARUSZENIE OCHRONY DANYCH OSOBOWYCH

LP.	Administrator (nazwa i dane kontaktowe)	Miejsce/ID zaistnienia naruszenia (nazwa i dane kontaktowe podmiotu przetwarzającego)	Okoliczności i charakter naruszenia	Konsekwencje naruszenia	Data wystąpienia naruszenia	Godz. wystąpienia naruszenia	Data stwierdzenia naruszenia	Godz. stwierdzenia naruszenia	Ilość osób	Ilość wpisów	Czy zgłoszono (TAK/NIE)	Powód zgłoszenia/braku zgłoszenia	Data i godz. zgłoszenia	Kategoria osób, których dotyczą dane	Zastosowane środki	Proponowane środki	Inspektor Ochrony Danych	Uwagi
	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	20

Nowy użytkownik **	Modyfikacja uprawnień **	Odebranie uprawnień w systemie **

Wzór karty zgłoszenia do systemu *

Dotyczy systemu: ……

(nazwa aplikacji (bazy danych), w której przetwarzane są dane)

Imię Użytkownika		
Jednostka i Komórka Organizacyjna		
Nazwisko Użytkownika		
Numer Pesel Użytkownika		
Numer telefonu wewnętrznego i adres e-mail		
Stanowisko		
Rodzaj umowy	**Data zakończenia obowiązywania umowy**(jeżeli umowa jest na czas określony)	
Posiada upoważnienie do przetwarzania danych osobowych:	**TAK**	**NIE**
Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie:		

*Przykład 1: Nazwa systemu ……SP W ROMANOWIE DOLNYM +Dostęp do jednostki „X” + odczyt dla jednostki „Y”.

*Przykład 2: Nazwa systemu ……SP W ROMANOWIE DOLNYM +Dostęp do jednostki „A” „B”„C”

Bezpośredni przełożony użytkownika systemu: (pieczęć i podpis)	Data:	
Inspektor Ochrony Danych: (pieczęć i podpis)	Data:	
Administrator Systemu Informatycznego:	Data:	Identyfikator systemu:

*Wypełniać drukowanymi literami

Numer wniosku: ……../201... r.

**Zaznaczyć jeden z wymienionych punktów

Załącznik Nr 12

Zgoda na przetwarzanie danych osobowych ucznia

w celu dokumentacji przebiegu procesu nauczania zgodnie z przepisami prawa, w tym także dokumentacji udziału ucznia w konkursach przedmiotowych oraz zawodach sportowych szkolnych i międzyszkolnych

…..……

Miejsce i data

Na podstawie art. 40 ust. 2 punkt f RODO oraz tzw. motywami w preambule RODO (motywy 38, 58, 71, 76) **j**a, niżej podpisana / podpisany*

……....……..……

imię, nazwisko *adres*

niniejszym wyrażam zgodę / nie wyrażam zgody* na nieograniczone czasowo/ ograniczone czasowo* tj. do dnia zakończenia procesu edukacji w Szkole Podstawowej w Romanowie Dolnym, na przetwarzanie danych osobowych mojego dziecka / podopiecznego

.....

imię, nazwisko

w zakresie dokumentacji przebiegu procesu nauczania, w tym także dokumentacji udziału w konkursach przedmiotowych oraz zawodach sportowych szkolnych i międzyszkolnych w postaci wpisów do dokumentacji procesu nauczania oraz innej dokumentacji świadczącej o aktywności szkolnej i międzyszkolnej przez

(pieczęć Szkoły Podstawowej w Romanowie Dolnym, Romanowo Dolne 124, 64-700 Czarnków z pełną nazwą i adresem)

zwaną dalej „SP w Romanowie Dolnym ”, w tym w szczególności na potrzeby:

a) dokonywania wpisów do dziennika zajęć,
b) sporządzania protokołów sprawdzianów wiadomości i umiejętności,
c) sporządzania protokołów zebrań Rady Pedagogicznej,
d) udziału w konkurach przedmiotowych szkolnych i pozaszkolnych,
e) udziału w zawodach sportowych, organizowanych przez SP w Romanowie Dolnym i poza szkołą,
f) udziału w innych wydarzeniach organizowanych przez SP w Romanowie Dolnym w celu realizacji procesu edukacji,
g) archiwum Szkoły Podstawowej w Romanowie Dolnym.

…….……

Czytelny podpis Opiekuna

*niepotrzebne skreślić

Załącznik Nr 13

Zgoda na przetwarzanie wizerunku ucznia w celach promocyjnych

…..……

Data i miejsce

Na podstawie art. 40 ust. 2 punkt f RODO oraz tzw. motywami w preambule RODO (motywy 38, 58, 71, 76) **ja**, niżej podpisana / podpisany*

……..…….……

imię, nazwisko, adres

niniejszym wyrażam zgodę / nie wyrażam zgody* na nieograniczone czasowo / ograniczone czasowo* do dnia zakończenia procesu edukacji w Szkole Podstawowej w Romanowie Dolnym, przetwarzanie danych osobowych mojego dziecka/podopiecznego

.....

imię i nazwisko

w zakresie wizerunku w postaci fotografii, fotografii cyfrowej, filmu w formie pliku multimedialnego / cyfrowego przez

(pieczęć Szkoły Podstawowej w Romanowie Dolnym z pełną nazwą i adresem)

zwaną dalej „SP w Romanowie Dolnym ”, w tym w szczególności na potrzeby działalności promocyjno-marketingowej Szkoły Podstawowej w Romanowie Dolnym, Romanowo Dolne 124, 64-700 Czarnków prowadzonej za pośrednictwem:

- gazetki/ tablicy Szkoły Podstawowej w Romanowie Dolnym,
- strony internetowej Szkoły Podstawowej w Romanowie Dolnym,
- mediów społecznościowych prowadzonych przez SP w Romanowie Dolnym (tj. Facebook, Twitter, itp.).

…….……

czytelny podpis Rodzica /Opiekuna

*niepotrzebne skreślić