POLITYKA OCHRONY DANYCH OSOBOWYCH DLA SZKOŁY PODSTAWOWEJ NR 1 IM. MARII DĄBROWSKIEJ WE WROCŁAWIU

UL. NOWOWIEJSKA 78, 50-315 WROCŁAW

WROCŁAW 2018

ROZDZIAŁ I:
WPROWADZENIE

I. Niniejsza Polityka Ochrony Danych Osobowych stanowi zestawienie opisów, procedur, rejestrów, analiz oraz wzorów klauzul informacyjnych, upoważnień, umów powierzenia, których posiadanie i stosowanie w bieżącej działalności przez Szkołę Podstawową nr 1 we Wrocławiu jest wymogiem wynikającym z przepisów 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 (dalej: RODO).

II. Polityka Ochrony Danych Osobowych uwzględnia wymogi wynikające z przepisów RODO, polskiej ustawy z dnia 10 kwietnia 2018 roku o ochronie danych osobowych (dalej: Ustawa) oraz przepisów szczególnych. Polityka powinna podlegać okresowym aktualizacjom w miarę rozwoju prawa ochrony danych osobowych i praktyki jego stosowania w Polsce oraz w Unii Europejskiej.

III. Na Politykę Ochrony Danych Osobowych Szkoły Podstawowej nr 1 we Wrocławiu składają się:

oraz załączniki:

1. Rejestr czynności przetwarzania danych;
2. Wzory upoważnień do przetwarzania danych;
3. Instrukcja postępowania w obszarze ochrony danych osobowych;
4. Procedura na wypadek kontroli ze strony Prezesa Urzędu Ochrony Danych Osobowych;
5. Wzory klauzul informacyjnych stosowanych w codziennej praktyce Szkoły Podstawowej;
6. Wzory oświadczeń o zgodzie dla sytuacji, gdy przetwarzanie odbywa się na tej podstawie;
7. Wzory umów powierzenia przetwarzania danych osobowych dla typowych przypadków działalności Szkoły Podstawowej;
8. Wzór umowy udostępnienia danych osobowych;
9. Wzory dokumentów związanych z organizowaniem konkursów przez Szkołę.

IV. Z uwagi na intensywny rozwój dziedziny ochrony danych osobowych, w tym planowane uchwalenie nowego rozporządzenia o e-prywatności, niniejsza Polityka Ochrony Danych

Osobowych powinna być poddawana okresowym weryfikacjom pod kątem jej aktualności oraz kompletności.

V. Pełna Polityka Ochrony Danych Osobowych uwzględniająca wszystkie dokumenty, o których mowa w pkt III powyżej, prowadzona jest przez Szkołę Podstawową w formie elektronicznej, dostępnej na każde zawołanie. Taka forma dokumentacji ułatwia zapoznawanie się z nią przez osoby upoważnione do przetwarzania danych osobowych w Szkole Podstawowej, ułatwia jej stosowanie w praktyce (w szczególności wzory dokumentów), jak również ułatwia dokonywanie jej zmiany w miarę zmieniającego się otoczenia, przepisów oraz przyjętych w Szkole Podstawowej rozwiązań technicznych i organizacyjnych przetwarzania danych osobowych.

ROZDZIAŁ II:
Szkoła Podstawowa nr 1 im. Marii Dąbrowskiej we Wrocławiu - OGÓLNA CHARAKTERYSTYKA DZIAŁALNOŚCI

A. Podstawy prawne działalności Szkoły

Szkoła Podstawowa nr 1 im. Marii Dąbrowskiej we Wrocławiu ul. Nowowiejska 78, 50-315 Wrocław jest publiczną jednostką oświatową Gminy Wrocław. **Działa na podstawie obowiązujących przepisów prawa, w tym w szczególności na podstawie:**

1. ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe;
2. ustawa z dnia 7 września 1991 roku o systemie oświaty;
3. rozporządzenie Ministra Edukacji Narodowej z 17 marca 2017 r. w sprawie szczegółowej organizacji publicznych szkół i publicznych przedszkoli;
4. rozporządzenie Ministra Edukacji Narodowej z 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły policealnej;
5. rozporządzenie Ministra Edukacji Narodowej z 7 czerwca 2017 r. zmieniające rozporządzenie w sprawie warunków i sposobu organizowania religii w publicznych przedszkolach i szkołach;
6. rozporządzenie Ministra Edukacji Narodowej z 25 sierpnia 2017 r. w sprawie zasad organizacji i udzielania pomocy psychologiczno-pedagogicznej w publicznych przedszkolach i szkołach;
7. swojego aktu założycielskiego oraz swojego statutu.

B. Cele działalności Szkoły

Celem działalności Szkoły Podstawowej jest zapewnienie warunków wszechstronnego rozwoju uczniów, osiąganego poprzez realizację zadań w zakresie nauczania, kształcenia umiejętności oraz wychowania, z uwzględnieniem zasad bezpieczeństwa, a także zasad promocji i ochrony zdrowia.

Cele te Szkoła osiąga m.in. poprzez:

1. prowadzenie dziecka do nabywania i rozwijania umiejętności wypowiadania się, czytania i pisania, wykonywania elementarnych działań arytmetycznych;
2. posługiwanie się prostymi narzędziami oraz kształtowanie nawyków społecznego współżycia;
3. rozwijanie możliwości poznawczych uczniów tak, aby mogli oni przechodzić od dziecięcego do bardziej dojrzałego i uporządkowanego rozumienia świata;
4. rozwijanie i przekształcanie spontanicznej motywacji poznawczej w motywację świadomą, przygotowującą do podejmowania zadań wymagających systematycznego i dłuższego wysiłku intelektualnego i fizycznego;
5. rozbudzanie i rozwijanie wrażliwości estetycznej i moralnej dziecka oraz jego indywidualnych zdolności twórczych;

6. wzmacnianie wiary dziecka we własne siły i zdolności;
7. kształtowanie potrzeby i umiejętności dbania o własne ciało, zdrowie i sprawność fizyczną;
8. wyrabianie czujności wobec zagrożeń dla zdrowia fizycznego i psychicznego;
9. wzmacnianie poczucia tożsamości kulturowej, historycznej, etnicznej i narodowej;
10. stwarzanie warunków do rozwoju wyobraźni i ekspresji werbalnej, plastycznej, muzycznej i ruchowej;
11. stwarzanie możliwości nabywania umiejętności nawiązywania i utrzymywania poprawnych kontaktów z innymi dziećmi, dorosłymi i osobami niepełnosprawnymi, przedstawicielami innych narodowości i ras;
12. uwzględnianie indywidualnych potrzeb dziecka i zapewnienie mu równych szans;
13. stwarzanie warunków do rozwijania samodzielności, obowiązkowości, podejmowania odpowiedzialności za siebie i najbliższe otoczenie;
14. kształtowanie umiejętności działania w rożnych sytuacjach szkolnych i pozaszkolnych;
15. uczenie właściwych zachowań w stosunku do zwierząt i otaczającej przyrody;
16. rozwijanie wrażliwości na cierpienie i przejawy niesprawiedliwości;
17. współdziałanie ze stowarzyszeniami i innymi organizacjami w zakresie działalności innowacyjnej;
18. przygotowanie uczniów do podjęcia decyzji o dalszym kształceniu i przyszłej aktywności zawodowej.

C. Kategorie osób, których dane są przetwarzane przez Szkołę

W obszarze przetwarzania danych osobowych działalność Szkoły Podstawowej nr 1 we Wrocławiu skupia się na przetwarzaniu danych osobowych:

1. dzieci aplikujących do uczęszczania do Szkoły Podstawowej oraz ich rodziców lub opiekunów prawnych;
2. uczniów uczęszczających do Szkoły Podstawowej oraz ich rodziców lub opiekunów prawnych;
3. uczniów biorących udział w konkursach i olimpiadach organizowanych przez Szkołę;
4. absolwentów Szkoły Podstawowej oraz ich rodziców lub opiekunów prawnych;
5. kadry pedagogicznej odpowiedzialnej za edukację dzieci uczęszczających do Szkoły Podstawowej;
6. kadry administracyjnej odpowiedzialnej za bieżące funkcjonowanie Szkoły Podstawowej;
7. innych osób z najbliższego otoczenia Szkoły Podstawowej – najemców pomieszczeń Szkoły, dostawców, wykonawców, kandydatów do pracy.

D. Szkoła jako administrator czy jako procesor

Z uwagi na fakt, że Szkoła Podstawowa nr 1 we Wrocławiu świadczy usługi edukacyjne w wykonaniu postanowień aktu założycielskiego, statutu oraz powszechnie obowiązujących przepisów prawa, które nakładają na nie określone obowiązki, należy uznać, że w świetle art. 4 pkt 7 RODO to Szkoła Podstawowa nr 1 we Wrocławiu odpowiada za cele i sposoby przetwarzania danych osobowych. Tym

samym generalnie w procesach przetwarzania danych realizowanych w swojej działalności Szkoła Podstawowa nr 1 we Wrocławiu będzie uznawana za administratora danych osobowych.

Na zasadzie wyjątku Szkoła występuje jako procesor przetwarzający dane osobowe w przypadku:

1. zbierania w imieniu organizatorów formularzy udziału swoich uczniów w konkursie/olimpiadzie organizowanej przez inną jednostkę oświatową, kulturalną lub inny podmiot działający w interesie publicznym;
2. działania w porozumieniu z Gminą Wrocław, w związku z uzyskiwaniem dofinansowania ze środków unijnych, krajowych lub wojewódzkich, gdzie Szkoła występuje jako podmiot przetwarzający dane na rzecz Beneficjenta i dalej, na rzecz Instytucji Pośredniczącej.

E. Powierzanie danych osobowych podwykonawcom

Zgodnie z artykułem 28 Ogólnego Rozporządzenia o Ochronie Danych Osobowych jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą. Przetwarzanie danych osobowych przez podmiot przetwarzający może odbywać się wyłącznie na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora.

RODO w art. 28 ust. 3 określa szczegółowe wymagania jakie powinna określać odpowiednio sformułowana umowa przetwarzania danych osobowych. Co istotne RODO w swojej treści nie posługuje się pojęciem „Umowy powierzenia", znanym z art. 31 ustawy o ochronie danych osobowych z 1997 roku, jednocześnie nazewnictwo takie zostało przyjęte przez Szkołę Podstawową nr 1 im. Marii Dąbrowskiej we Wrocławiu w związku z obowiązującą na rynku utrwaloną praktyką w tym obszarze.

W toku audytu w Szkole Podstawowej zidentyfikowano, że Szkoła Podstawowa generalnie nie jest podmiotem przetwarzającym dane (sytuacje takie mogą zdarzać się jedynie wpadkowo; np. konkursy organizowane prze inne placówki oświatowe), a generalnie dla swoich procesów jest administratorem danych, który powierza przetwarzanie danych osobowych innym podmiotom.

Zidentyfikowano następujące obszary, w których Szkoła Podstawowa trwale lub często powierza przetwarzanie danych osobowych:

1. Obsługa IT
2. Obsługa w obszarze BHP
3. Obsługa prawna
4. Utylizacja dokumentów
5. Obsługa strony www
6. Korzystanie z oprogramowania bazodanowego
7. Realizacja wydruków masowych

8. Usługi archiwizacji dokumentów
9. Usługi fotografa

Dla powyższych przypadków Szkoła Podstawowa posiada opracowany zestaw wzorów umów powierzenia przetwarzania danych osobowych, które składają się na Politykę Ochrony Danych Osobowych.

F. Udostępnianie danych przez Szkołę innym podmiotom

Działalność Szkoły Podstawowej nr 1 we Wrocławiu nie wiąże się z koniecznością przetwarzania danych osobowych na masową skalę. Szkoła Podstawowa nie udostępnia danych osobowych innym podmiotom w celach komercyjnych. Pozostaje jednak jednostką oświatową Gminy Wrocław i jest zobowiązana do przekazywania określonych raportów oraz informacji do poszczególnych Wydziałów Gminy Wrocław, zgodnie z powszechnie obowiązującymi przepisami prawa oraz regulacjami prawa miejscowego.

Ponadto udostępnianie danych osobowych ma również miejsce w przypadku podejmowania przez Szkołę współpracy z ośrodkami medycznymi, które angażują się w określone badania zdrowotne uczniów (np. wszawica, choroby skórne, uzębienie). W tych przypadkach administratorem danych osobowych jest podmiot przeprowadzający dane badanie, działający za zgodą Szkoły oraz rodziców lub przedstawicieli prawnych uczniów.

G. Zidentyfikowane w Szkole procesy przetwarzania danych

W toku audytu zidentyfikowano w Szkole następujące procesy przetwarzania danych osobowych:

KATEGORIA PROCESU	PROCES	NUMER PORZĄDKOWY
FAKTURY	Faktury sprzedażowe i noty księgowe	1.
	Faktury zakupowe i noty księgowe	2.
UMOWY	Umowy zakupu	3.
	Umowy najmu	4.
	Pozostałe umowy	5.
ZATRUDNIENIE	Rekrutacja	6.
	Dane pracowników	7.
	Dokumentacja awansu zawodowego nauczyciela	8.
	Rada Pedagogiczna	9.
	Fundusz Świadczeń Socjalnych	10.
	Wypadki pracowników przy pracy lub w drodze do pracy	11.
UCZNIOWIE	Rekrutacja uczniów	12.
	Świadczenie działalności edukacyjnej	13.
	Wyżywienie	14.
	Świetlica	15.
	Egzamin ósmoklasisty	16.

	Rejestr absolwentów i świadectw szkolnych	17.
	Rejestr wypadków uczniów	18.
	Wycieczki	19.
	Konkursy	20.
	Biblioteka	21.
	Pomoc psychologiczno -pedagogiczna	22.
KOMUNIKACJA	Korespondencja e-mail	23.
	Tablice Szkolne	24.
	Gazetka Szkolna	25.
	Strona www	26.
	Rada Rodziców	27.
	Kurierzy i Poczta Polska	28.
ADMINISTRACJA	Rejestry kontroli organów i urzędów	29.
	Rejestr wejść i wyjść	30.
	Monitoring wizyjny	31.
	Postępowania przed sądami i organami administracji	32.
DOKUMENTACJA WEWNĘTRZNA	Obsługa administracyjna	33.
	Rejestr incydentów w obszarze ochrony danych osobowych	34.

Powyższe procesy przetwarzania danych osobowych realizowane przez Szkołę Podstawową nr 1 im. Marii Dąbrowskiej we Wrocławiu zostały dokładnie opisane w ramach Rejestru Czynności, który stanowi Załącznik nr 1 do niniejszej Polityki. Ten opis czynności stanowi również podstawę dla opracowanych upoważnień do przetwarzania danych osobowych dla pracowników Szkoły Podstawowej (Załącznik nr 2).

H. Przetwarzanie przez Szkołę danych wrażliwych

Przetwarzane przez Szkołę Podstawową nr 1 im. Marii Dąbrowskiej we Wrocławiu dane osobowe generalnie nie mają charakteru wrażliwego. Dane wrażliwe pojawiają się jednak w przypadku, gdy uczniowie mają jakieś schorzenia lub przewlekłe choroby (w tym psychiczne), w przypadkach, gdy rodzice deklarują chęć brania przez dziecka udziału w zajęciach religii, w obszarze przetwarzania danych osobowych pracowników w zakresie ich zdrowotnych zdolności do pracy – w zakresie wymaganym przez przepisy polskiego prawa. Elementy danych wrażliwych pojawiają się również w tym przypadkach, gdzie Szkoła aktywnie działa w zakresie wsparcia psychologiczno-pedagogicznego i w tym zakresie pozyskuje dodatkowe dane o uczniu i/lub jego sytuacji rodzinnej. W przypadkach trudnych uczeń kierowany jest jednak do odrębnej od Szkoły placówki – Poradni Psychologiczno – Pedagogicznej funkcjonującej na terenie Wrocławia.

I. Zaświadczenia o niekaralności

Wymaga wskazania, że w przypadku zatrudniania osób na stanowiska nauczycieli, zgodnie z art. 10 ust. 5 ustawy – Karta nauczyciela, zbierane są od przyszłych pracowników zaświadczenia o niekaralności wydawane przez Krajowy Rejestr Karny. Nadto w świetle art. 10 ust. 8b Karty Nauczyciela, dyrektor szkoły, przed nawiązaniem stosunku pracy z nauczycielem, jest obowiązany zasięgnąć informacji z Centralnego Rejestru Orzeczeń Dyscyplinarnych, prowadzonego przez Ministra Edukacji Narodowej, czy nauczyciel nie był karany karą administracyjną, o której mowa w art. 10 ust. 5 pkt 4a Karty Nauczyciela. Tym samym Szkoła Podstawowa zbiera w swoich systemach ww. dane mające charakter wrażliwy z powołaniem na art. 9 ust. 2 lit. b) RODO.

J. Spełnianie obowiązku informacyjnego przez Szkołę

Zgodnie z art. 13 i 14 Ogólnego Rozporządzenia o Ochronie Danych Szkoła Podstawowa nr 1 we Wrocławiu ma obowiązek informować osoby, których dane dotyczą, o fakcie i sposobach przetwarzania ich danych osobowych przez jednostkę. Określony powyżej obowiązek informacyjny jest jednym z najważniejszych obowiązków nakładanych przez RODO, które kładzie istotny nacisk na transparentność w procesach przetwarzania danych osobowych.

W stosunku do wcześniejszych regulacji ustawy o ochronie danych osobowych z 1997 roku, RODO wprowadza bardzo szeroki katalog informacji, które należy przekazywać osobom, których dane dotyczą. Obowiązek ten należy realizować w każdym przypadku, gdy dane są uzyskiwane bezpośrednio od osoby, której dane dotyczą. Obowiązek ten należy również realizować w większości przypadków, gdy dane są zbierane od osoby trzeciej lub z innych źródeł (z wyłączeniem przypadków określonych w art. 14 ust. 5 RODO).

W procesie audytu w Szkole określono następujące przypadki zbierania danych osobowych, które wiążą się z obowiązkiem przedstawienia osobom, których dane dotyczą klauzul informacyjnych:

1. osoby, z którymi Szkoła Podstawowa nr 1 we Wrocławiu koresponduje za pośrednictwem poczty elektronicznej – w tych przypadkach Szkoła Podstawowa nr 1 we Wrocławiu zbiera takie dane jak adresy e-mail, treść korespondencji, dane kontaktowe podawane w stopkach respondentów;
2. petenci składający różnego rodzaju pisma w placówce – Szkoła Podstawowa nr 1 we Wrocławiu zbiera dane osobowe, które są zawarte w takim piśmie; dokładny zakres danych, który może być zawarty w takim piśmie jest trudny z góry do określenia, dlatego też klauzula informacyjna w tym obszarze musi być odpowiednio szeroka;
3. osoby korzystające ze strony internetowej placówki – zbieranie m.in. ciasteczek, które na gruncie RODO zostały uznane za dane osobowe;
4. przyjmowanie aplikacji rekrutacyjnych dzieci do Szkoły Podstawowej – zbieranie danych o dzieciach oraz ich rodzicach lub opiekunach prawnych;
5. zbieranie informacji o osobach uprawnionych przez rodziców lub opiekunów prawnych do odbioru dziecka ze świetlicy – klauzula przedstawiana jest osobie, której dane dotyczą przy okazji jej najbliższej wizyty w Szkole Podstawowej w celu odbioru dziecka;
6. zbieranie danych osobowych kandydatów do pracy oraz w związku z zatrudnieniem (w przypadku pozytywnej rekrutacji);

7. zbieranie danych w związku z wykorzystywaniem w Szkole Podstawowej monitoringu wizyjnego – klauzula wywieszana jest na tablicy na terenie Szkoły Podstawowej; nadto zastosowano oznaczenia graficzne.

Klauzule informacyjne dla powyższych przypadków zostały ujęte w Załączniku nr 5 do niniejszej Polityki Ochrony Danych Osobowych prowadzonej przez Szkołę Podstawową nr 1 im. Marii Dąbrowskiej we Wrocławiu .

K. Przypadki, dla których zidentyfikowano obowiązek uzyskania zgody na przetwarzanie danych osobowych przez Szkołę Podstawową nr 1 im. Marii Dąbrowskiej we Wrocławiu

Artykuł 6 Ogólnego Rozporządzenia o Ochronie Danych przewiduje sześć różnych podstaw prawnych przetwarzania danych osobowych. Szkoła Podstawowa nr 1 im. Marii Dąbrowskiej we Wrocławiu jako jednostka publiczna nie może korzystać z podstawy prawnej przetwarzania, jaką jest uzasadniony interes administratora danych osobowych (art. 6 ust. 1 lit. f).

Co do zasady Szkoła Podstawowa nr 1 im. Marii Dąbrowskiej we Wrocławiu na co dzień przetwarza dane osobowe z powołaniem na następujące podstawy przetwarzania:

1. Wykonanie umowy (art. 6 ust. 1 lit. b RODO)
2. Wykonanie obowiązku wynikającego z przepisu prawa (art. 6 ust. 1 lit. c RODO)
3. Działanie w wykonaniu władzy publicznej lub w interesie publicznym (art. 6 ust. 1 lit e RODO).

Działania z powołaniem na zgodę osoby, której dane dotyczą lub z powołaniem na ochronę żywotnych interesów osoby, której dane dotyczą, będą miały charakter wyjątkowy.

Działania z powołaniem na ochronę żywotnych interesów mają charakter wyjątkowy z tej przyczyny, że ta podstawa prawna dotyczy wpadkowych sytuacji, niecierpiących zwłoki, w których interesy jednostki przeważają w danej chwili nad ochroną jej prywatności. Jednocześnie administrator powinien w pierwszej możliwej chwili, kiedy tylko oddalone zostanie ryzyko dla interesów jednostki, znaleźć inną podstawę prawną przetwarzania.

W przypadku zgody jako podstawy prawnej przetwarzania, ma ona dla działalności Szkoły Podstawowej charakter wyjątkowy, ponieważ Szkoła Podstawowa działając jako organ publiczny działa generalnie z powołaniem na klauzulę przepisów prawa lub interesu publicznego. Jednocześnie w toku audytu w Szkole Podstawowej zdiagnozowano przypadki działania w granicach interesu publicznego (funkcja wychowawcza Szkoły Podstawowej, kształtowanie społeczności lokalnej, wykonywanie funkcji informacyjnej), które jednak mogą istotnie wpływać na prawa i interesy osób, których dane dotyczą.

Chodzi tutaj o przypadki publikowania wizerunków uczniów i rodziców w sieci Internet. Działania takie, chociaż uzasadnione klauzulą interesu publicznego, wiążą się z upublicznieniem danych

osobowych w taki sposób, że osoby, których dane dotyczą mogą utracić kontrolę nad ich rozprzestrzenianiem się. Z tych przyczyn Szkoła Podstawowa nr 1 im. Marii Dąbrowskiej we Wrocławiu zdecydowała się dla tych przypadków przetwarzania danych uzyskiwać odrębną zgodę od osób, których dane dotyczą.

Zupełnie odrębnym przypadkiem, jest standardowo występująca w polskich Szkołach Podstawowych zgoda rodziców na udział ich dziecka w zajęciach religii. Oświadczenie takie ma charakter zgody, jednak jest to zgoda dotycząca udziału w zajęciach religii, a nie zgoda na przetwarzanie danych osobowych w związku z udziałem w takich zajęciach. W analizowanym przypadku podstawą prawną przetwarzania danych osobowych dzieci są przepisy Rozporządzenia Ministra Edukacji Narodowej z dnia 14 kwietnia 1992 r. w sprawie warunków i sposobu organizowania nauki religii w publicznych przedszkolach i szkołach. Jeżeli rodzic, w trybie przewidzianym przez przepisy ww. Rozporządzenia, wyrazi wolę udziału swojego dziecka w zajęciach religii, to Szkoła Podstawowa co do zasady jest zobowiązana zapewnić udział dziecka w zajęciach religii. Podstawą prawną przetwarzania danych osobowych dziecka w tym zakresie będzie art. 9 ust. 2 lit. g) RODO, zgodnie z którym przetwarzanie danych osobowych wrażliwych jest uprawnione w przypadku, gdy:

- *przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą*.

Treść zbieranych zgód na przetwarzanie danych osobowych została określona w niniejszej Polityce Ochrony Danych Osobowych Szkoły Podstawowej nr 1 im. Marii Dąbrowskiej we Wrocławiu . Z przyczyn porządkowych oświadczenie o woli udziału dziecka w zajęciach religii wraz ze stosowną klauzulą informacyjną również umieszczono w Polityce Ochrony Danych Osobowych. Wzorcowa treść klauzul zgody stanowi Załącznik nr 6 do niniejszej Polityki Ochrony Danych Osobowych.

L. Organizacja konkursów przez Szkołę

Uczniowie Szkoły Podstawowej mogą brać udział w wielu konkursach w trakcie roku szkolnego. Część konkursów ma charakter wewnętrzny (tylko dla uczniów Szkoły), a część konkursów ma charakter międzyszkolny (regionalny, ponadregionalny, ogólnopolski).

Dla przypadków konkursów wewnętrznych Szkoła nie musi realizować żadnych dodatkowych czynności w obszarze przetwarzania danych osobowych. W tym zakresie, zgodnie z Testem klauzuli interesu publicznego (Rozdział IV Polityki Ochrony Danych Osobowych) Szkoła działa w granicach swojej misji edukacyjnej, a podejmowane czynności przetwarzania danych osobowych nie wykraczają poza bieżące funkcjonowanie placówki.

W przypadku pozostałych konkursów sytuacja przedstawia się już nieco inaczej. Tam gdzie Szkoła jako organizator konkursu zbiera dane osobowe uczniów innych placówek w celu realizacji konkursu, powinna uzyskać odrębną zgodę rodziców/przedstawicieli ustawowych uczniów na ich udział w konkursie. Taka zgoda w świetle art. 6 ust.1 lit. a RODO będzie oznaczała również zgodę na

przetwarzanie danych osobowych tych uczniów w celu realizacji konkursu. Przy okazji zbierania takiej zgody Szkoła zobowiązana jest wypełnić obowiązek informacyjny w rozumieniu art. 13 RODO. Jeżeli dodatkowo Szkoła planuje publikować zdjęcia z przebiegu konkursu w Internecie, w mediach społecznościowych, zobowiązana jest uzyskać na to odrębną zgodę.

W praktyce funkcjonowania jednostek oświatowych w konkursach międzyszkolnych występują etapy wewnątrzszkolne oraz etapy ponad szkolne. Szkoła – organizator potrzebuje uzyskiwać dane wyłącznie tych uczniów, których dana Szkoła – uczestnik zgłasza do udziału w etapie ponad szkolnym konkursu. Szkoła – organizator na żadnym etapie nie przetwarza danych osobowych uczniów, którzy nie przeszli do etapu ponad szkolnego.

Jak wskazano powyżej, Szkoła - organizator ma obowiązek uzyskiwać zgody rodziców / przedstawicieli ustawowych na udział dziecka w konkursie. Powinna również wypełnić obowiązek informacyjny. W praktyce działania te są realizowane za pośrednictwem dedykowanego formularza. Wzór takiego formularza został określony w Załączniku nr 9a. do niniejszej Polityki Ochrony Danych Osobowych.

Obowiązek przedstawienia formularza rodzicom/przedstawicielom ustawowym, oraz zapewnienie jego podpisania ciąży zazwyczaj na Szkole – uczestniku, która następnie ma obowiązek przekazać odpowiednio wypełniony formularz Szkole – organizatorowi. Taka praktyka w świetle art. 28 RODO oznacza, że Szkoła – uczestnik w zakresie w jakim zapewnia wypełnienie formularza zgody na udział ucznia w międzyszkolnym etapie Konkursu działa jako podmiot przetwarzający dane osobowe na rzecz Szkoły – organizatora. W świetle art. 28 ust. 3 RODO taka sytuacja oznacza, że Szkoła – organizator powinna zapewnić podpisanie umowy powierzenia przetwarzania danych osobowych ze wszystkimi Szkołami – uczestnikami, albo powinna w tym zakresie wykorzystać tzw. „inny instrument prawny". Z uwagi na trudności organizacyjne związane z zapewnieniem podpisania tak dużej ilości umów powierzenia przetwarzania danych osobowych w ciągu roku, w ramach Polityki Ochrony Danych Osobowych w Szkole przyjęto formułę stosowana „innego instrumentu prawnego", jakim jest odrębny załącznik do regulaminu Konkursu, który przewiduje określone zobowiązania w obszarze ochrony danych osobowych (spełniające kryteria art. 28 ust. 3 RODO) dla wszystkich Szkół, które zdecydują się wziąć udział w Konkursie. Wzór stosowanego załącznika do regulaminu konkursu stanowi Załącznik nr 9b. do niniejszej Polityki Ochrony Danych Osobowych.

Każda Szkoła – uczestnik przystępując do udziału w Konkursie organizowanego przez Szkołę równocześnie akceptuje obok regulaminu samego konkursu również reguły przetwarzania danych osobowych z nim związanych. W ten sposób spełnione są warunki powierzenia przetwarzania danych określone przez art. 28 RODO.

M. Status Rady Rodziców

Szczególne wątpliwości w świetle praktyki stosowania RODO na gruncie polskiego prawa budzi status Rady Rodziców w strukturze jednostki oświatowej. Z jednej strony wskazuje się, że Rada Rodziców jest jedynie wewnętrznym organem Szkoły Podstawowej, nie ma charakteru samodzielnego, nie

może być odrębnym podmiotem praw i obowiązków, nie istniałaby gdyby nie Szkoła. Z drugiej strony historycznie pojawiają się wypowiedzi i orzeczenia, które jednoznacznie wskazują, że Rada Rodziców w obszarze swoich kompetencji może samodzielnie decydować o celach i środkach przetwarzania danych osobowych, ponieważ jest w pewnym stopniu niezależna w obszarze swojej decyzyjności od dyrekcji placówki (np. decyzja Generalnego Inspektora Ochrony Danych Osobowych nr DOLiS/DEC – 769/08 z dnia 01 grudnia 2008 roku).

W celu zaadresowania tego problemu Szkoła Podstawowa nr 1 im. Marii Dąbrowskiej we Wrocławiu uznaje, że Rada Rodziców w obszarze swojej podstawowej działalności co do zasady nie spełnia kryteriów do uznania za odrębnego od Szkoły Podstawowej administratora danych (kryterium samodzielnego decydowania o celach i środkach przetwarzania danych osobowych co do zasady nie zostaje spełnione). Z tej perspektywy do wzorów upoważnień do przetwarzania danych osobowych dodano również upoważnienia do przetwarzania danych przez członków Rady Rodziców.

Jednocześnie w tym miejscu, podsumowując jedynie ten złożony problem należy wskazać, że Szkoła Podstawowa w określonych przypadkach będzie uznawać Radę Rodziców (jej członków działających w otoczeniu Szkoły) za odrębnego administratora danych, który jest obowiązany do samodzielnego zadbania o prawidłowość przetwarzania danych osobowych. Dotyczyć to będzie w szczególności:

1. przypadków, gdy sposób funkcjonowania Rady Rodziców w sposób istotny oddzieli się od Szkoły Podstawowej – w szczególności prace Rady Rodziców będą odbywały się poza placówką, poza placówką będzie przechowywana dokumentacja zawierająca dane osobowe, Rada Rodziców będzie odmawiać prawa do nadzoru Rady ze strony Inspektora Ochrony Danych Osobowych lub będzie odmawiać zastosowania się do jego wskazań;
2. dla procesów przetwarzania, w których Rada Rodziców będzie działała całkowicie z własnej inicjatywy poza auspicjami Szkoły Podstawowej – np. prowadzenie samodzielnego profilu w mediach społecznościowych (np. fanpage Rady Rodziców na Facebook'u) lub inne przypadki samodzielnego publikowania danych osobowych (uczniów, nauczycieli).

N. Rozwiązania informatyczne

Szkoła Podstawowa nie wykorzystuje zaawansowanych systemów informatycznych do przetwarzania danych osobowych. Nie tworzy również systemów typu Big Data. Przetwarzanie odbywa się z wykorzystaniem tradycyjnych rozwiązań papierowych, jak również z wykorzystaniem rozwiązań informatycznych przyjętych przez jednostkę, tj.:

1. **Dziennik Elektroniczny** – zapewniany Szkole przez zewnętrzną firmę Vulcan / Librus / xxxxxx;
2. Oprogramowanie wspierające w **zarządzaniu kadrami** – Vulcan / Librus / xxxxx ;
3. **Portal Wrocławska Edukacja** – którego funkcjonalności obejmują pocztę elektroniczną, elektroniczny kalendarz, dziennik elektroniczny, platformy edukacyjne;
4. **Zintegrowany System Zarządzania Wrocławską Oświatą** – zawierający funkcjonalności wspierające zarządzanie Szkołą Podstawową. Służy jako hurtowania danych o rodzicach, dzieciach, pracownikach jednostki;

5. System Informacji Oświatowej Ministerstwa Edukacji Narodowej – polski, elektroniczny system baz danych służący do gromadzenia informacji o szkołach, placówkach oświatowych, nauczycielach oraz uczniach, utworzony na podstawie:
    a. ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej,
    b. rozporządzenia Ministra Edukacji Narodowej z dnia 9 sierpnia 2012 r. w sprawie szczegółowego zakresu danych gromadzonych w bazach danych oświatowych, zakresu danych identyfikujących podmioty prowadzące bazy danych oświatowych, terminów przekazywania danych między bazami danych oświatowych oraz wzorów wydruków zestawień zbiorczych;
6. Szkoła Podstawowa posiada swoją stronę internetową www.sp1.wroclaw.pl;
7. Za obsługę informatyczną Szkoły Podstawowej odpowiada wrocławskie Centrum Usług Informatycznych;
8. Szkoła Podstawowa posiada swój profil w mediach społecznościowych: FEJSBUK.

ROZDZIAŁ III:
OGÓLNA ANALIZA RYZYKA DLA PROCESÓW PRZETWARZANIA W SZKOLE PODSTAWOWEJ NR 1 WE WROCŁAWIU

Ogólna analiza ryzyka dla ochrony danych osobowych w Szkole Podstawowej nr 1 im. Marii Dąbrowskiej we Wrocławiu została przeprowadzona z uwzględnieniem zasad określonych w Poradniku Prezesa Urzędu Ochrony Danych Osobowych w tym zakresie („Jak rozumieć podejście oparte na ryzyku? Poradnik RODO. Podejście oparte na ryzyku. Część 1", maj 2018, oraz „Jak stosować podejście oparte na ryzyku. Poradnik RODO. Podejście oparte na ryzyku. Część 2", maj 2018).

A. Określenie kryteriów akceptacji ryzyka

Dla potrzeb dokonywanej analizy ryzyka przyjęto następujące kryteria akceptacji ryzyka:

1. Poziom akceptowalny (0-2) - Brak ryzyka, ryzyko minimalne lub wystarczająco niskie, aby mogło uzyskać akceptację;
2. Poziom średni (3-6) - Ryzyko na poziomie średnim, co do którego należy przewidzieć obowiązek wprowadzenia czynników obniżających poziom ryzyka w czasie;
3. Poziom wysoki (7-9) - Ryzyko wysokie, nieakceptowalne. Wymagane jest przeprowadzenie Oceny Skutków dla Ochrony Danych i określenie sposobu niezwłocznego obniżenia ryzyka lub konieczna jest rezygnacja z danych działań.

B. Możliwe zagrożenia brane pod uwagę przy szacowaniu ryzyka

Przy szacowaniu ryzyka wzięto pod uwagę możliwość wystąpienia następujących zagrożeń dla ochrony danych osobowych przetwarzanych przez Szkołę:

ZAGROŻENIE	OPIS	RODZAJ ZAGROŻENIA
Phishing	Mail z prośbą o zalogowanie się do „podróbki" strony, np. bankowej, lub pseudo konta gmail i w rezultacie przejęcie hasła.	Ataki socjotechniczne
Cybersquatting	Zachęcanie do zalogowania się do podrobionej strony o „wiarygodnym" adresie www. Zamiast logować się do www.mbank.pl logowanie byłoby w www.rnbank.pl Faxy, w których intruz podszywa się pod dostawcę i informuje o zmianie numeru konta bankowego. Maile lub rozmowy tel., w których intruz podaje się np. za pracownika firmy dostarczającej oprogramowanie i prosi o hasło w celu „przetestowania uprawnień"	Ataki socjotechniczne
Nakłanianie do wykonania czynności	Maile, które zachęcają lub „zmuszają" do otwarcia załączników lub kliknięcia na hiperlink, wpisywanie komend	Ataki socjotechniczne
Podrzucone nośniki danych	Pen drive pozostawiony w biurze	Ataki socjotechniczne
Ataki telefoniczne	· Intruz przedstawia się jako pracownik dostawcy łącza naprawiający usterkę i prosi o uruchomienie określonej strony internetowej.	Ataki socjotechniczne

	· Intruz przedstawia się jako inżynier Microsoftu lub programista dostawcy oprogramowania. Podsyła „aktualizację” lub prosi o udostępnienie pulpitu	
Łamanie i pozyskiwanie haseł	· Łamanie metodami słownikowymi i siłowymi · Ujawnianie haseł · Nieprawidłowe przechowywanie (karteczki, pliki) · Odgadywanie zbyt słabych, najpopularniejszych haseł · Stosowanie domyślnych haseł producenta · Stosowanie słownikowych haseł (np. 8 znaków z 3 grup: „Grażynka1”) · Stosowanie jednego hasła do wielu (często wszystkich) systemów	Ataki na infrastrukturę
Ataki na sprzęt	Włamania do urządzeń nieaktualizowanych *Urządzenia sieciowe (routery, access pointy, firewalle) oraz inne np. macierze, dyski NAS działają dzięki umieszczonemu na nich oprogramowaniu. To oprogramowanie, jak każde inne podlega testom bezpieczeństwa i znajdowane są w nim dziury. Brak aktualizacji tego oprogramowania skutkuje podatnością na włamania, kradzież danych, zakłócanie pracy.* Włamania do urządzeń nieodpowiednio skonfigurowanych *Błędy konfiguracyjne popełniane przez administratorów mogą ułatwiać hackerom włamanie się do sieci lub urządzenia. Powodem jest najczęściej brak profesjonalnej wiedzy u osób konfigurujących urządzenia. Przykładem może być pozostawienie domyślnych haseł lub dostępu do strony konfiguracyjnej z poziomu Internetu.* Włamania z użyciem niezabezpieczonych interfejsów lokalnych *Urządzenia takie jak routery, switche, firewalle posiadają często porty konfiguracyjne (USB, Ethernet lub COM - szeregowe), które podłącza się do komputera aby skonfigurować urządzenie. Dostęp do tych portów powinien być odpowiednio zabezpieczonych hasłem, aby przypadkowa osoba, która podłączy do nich swój komputer nie mogła zmienić konfiguracji. Administratorzy często jednak pozostawiają te porty niezabezpieczone.* Włamania za pośrednictwem niepotrzebnych usług (np. telnet na routerze) *Urządzenia sieciowe posiadają często włączone wszystkie możliwe usługi sieciowe (DHCP, DNS, SSH, HTTP, telnet, FTP), mimo iż nie wszystkie z nich są potrzebne w danym środowisku. Każda z tych usług jest obsługiwana przez oprogramowanie, które może zawierać błędy. Wyłączenie niepotrzebnych serwisów ogranicza ilość dziur i możliwość przechwycenia / podsłuchania ruchu lub haseł. Włączone powinny być tylko te usługi, które są niezbędne do działania danego środowiska*.	Ataki na infrastrukturę
Ataki na oprogramowanie	Wykorzystanie znanych dziur w nieaktualizowanym oprogramowaniu *W każdym oprogramowaniu (przeglądarki, pakiety biurowe, systemy operacyjne, systemy serwerowe...) prędzej czy później znajdowane są błędy pozwalające na przełamania zabezpieczeń i uzyskanie zdalnego dostępu lub zdalne wykonanie kodu. Informacje o tych błędach są upubliczniane po tym, jak producent oprogramowania przygotuje odpowiednią łatę lub aktualizację. Jeżeli nie zainstalujemy tych aktualizacji, narażamy się na ryzyko, że ktoś wykorzysta ogólnodostępne informacje o znanych błędach aby włamać się, wykraść dane, lub w inny*	Ataki na infrastrukturę

	sposób nam zaszkodzić. (nieaktualizowany Windows 7) Włamania z wykorzystaniem luk typu zero day *Zero-day to błędy w oprogramowaniu, o których informacje zostają upublicznione zanim jeszcze autor oprogramowania zdąży wypuścić aktualizację. Często pojawiają się narzędzia umożliwiające wykorzystanie tych błędów (exploity) i przełamanie zabezpieczeń skutkujące włamaniem, kradzieżą danych itp. Innymi słowy - Zero day – podatność sprzętu lub oprogramowania znana wąskiej grupie osób i pozwalająca na przełamanie zabezpieczeń, na którą producent nie dostarczył jeszcze odpowiedniej aktualizacji* Włamania z wykorzystaniem domyślnych haseł *Włamania będące wynikiem tego, że administrator po uruchomieniu oprogramowania lub urządzenia nie zmienił domyślnego hasła. Intruz, któremu uda się rozpoznać model urządzenia w pierwszej kolejności próbuje się do niego zalogować hasłem podanym w instrukcji obsługi przez producenta. Często się to niestety udaje.* Włamania z wykorzystaniem najczęstszych błędów *Programiści pisząc oprogramowanie często popełniają te same znane błędy. Istnieje zestawienie takich błędów, np. dla aplikacji webowych - OWASP TOP 10. Wiele programów i stron internetowych pada ofiarą ataków właśnie za pośrednictwem tych najczęstszych błędów.* Włamania z wykorzystaniem API (interfejsów programistycznych) *Niektóre aplikacje, systemy ale też serwisy internetowe (np. Allegro) posiadają specjalne interfejsy, dzięki którym programiści używając odpowiednich bibliotek mogą odwoływać się do nich z poziomu oprogramowania, Możliwe jest np. wystawienie aukcji na allegro bez konieczności logowania się na swoje konto przeglądarką internetową. Błędy w tych bibliotekach powodowały często, że programista mógł np. uzyskać szerszy dostęp do bazy danych i wyciągnąć dane wszystkich klientów.* Namierzanie wersji testowych (np. strona www) *Niektóre portale lub aplikacje webowe posiadają swoje kopie utrzymywane do celów testowych lub rozwojowych. Programiści zamieszczają na nich zmiany w kodzie zanim trafią one na główne serwery. Strony te są często gorzej zabezpieczone i łatwiej jest się do nich włamać, a mogą zawierać również krytyczne dane. Często udaje się je namierzyć wpisując np. zamiast adresu www.strona.pl adres test.strona.pl .*	
Skanowanie sieci i usług	Atakujący poznaje wersję systemu operacyjnego lub wersję serwera www a przez to potem może dobrać skuteczny atak	Ataki na infrastrukturę
Podsłuchanie transmisji (okablowanie, wifi, telefonia, internet)	Łatwo dostępne gniazdka sieciowe, gdzie atakujący może się podłączyć np. z własnym urządzeniem i za jego pomocą podsłuchiwać naszą sieć (możliwość podpięcia się pod drukarkę na korytarzu lub do gniazdka w salce konferencyjnej)	Ataki na infrastrukturę
ATAKI MAN-IN-THE-MIDDLE	Przejęcie komputera w firmie w celu podsłuchiwania w sieci firmowej (w rezultacie możliwość podsłuchu haseł)	Ataki na infrastrukturę
Eskalacja uprawnień	• Zwiększenie uprawnień użytkownika przez wykorzystanie błędów programistycznych • Przejęcie uprawnień użytkownika zaawansowanego • Przejęcie uprawnień administratora	Ataki na infrastrukturę

	• Przejęcie uprawnień systemowych • Przejęcie innych poświadczeń (certyfikaty elektroniczne, pliki cookies z identyfikatorami sesji)	
DOS	Zmasowany atak pojedynczego atakującego na jakąś stronę www lub na portal, aby ją przeciążyć i „zakorkować”	Ataki na infrastrukturę
DDOS	Zmasowany atak komputerów-zombie na zlecenie atakującego na jakąś stronę www lub na portal, aby ją przeciążyć i „zakorkować”	Ataki na infrastrukturę
Wirusy i trojany	Trojany – instalują się często z nielegalnym oprogramowaniem. Zawierają ukrytą funkcjonalność, działają na szkodę użytkownika.	Złośliwe oprogramowanie
Backdoory	Instalują się z maili lub z linków w mailach. Po uruchomieniu umożliwiają intruzowi ponowny dostęp i stałą kontrolę nad komputerem. Taki komputer-zombie może być użyty do wszelkich zachcianek intruza.	Złośliwe oprogramowanie
Keyloggery	Programy przechwytujące hasła wpisywane na klawiaturze przez użytkownika i oddające je intruzowi.	Złośliwe oprogramowanie
Ransomeware	Program do szyfrowania plików. Odszyfrowanie wymaga zapłaty 500 USD. Bardzo groźny	Złośliwe oprogramowanie
Exploity / exploitpaki	Oprogramowanie wykorzystujące znane luki w systemach. Uruchomiony pozwala na przejęcie systemu przez intruza.	Złośliwe oprogramowanie
Włamanie do obiektów	Może skutkować zainstalowaniem nieautoryzowanych urządzeń, np. keyloggerów, podsłuchów	Zagrożenia dla sprzętu
Kradzież / zniszczenie sprzętu	Kradzież komputerów w organizacji i laptopów poza nią, uszkodzenie sprzętu na skutek przepięcia, czy upadku	Zagrożenia dla sprzętu
Pożar / eksplozja	Np. pożar serwerowni, wybuch gazów technicznych	Zagrożenia dla sprzętu
Zalanie	Np. powódź, pęknięta rura kanalizacyjna, zalanie kawą	Zagrożenia dla sprzętu
Przegrzanie	Wysoka temperatura w serwerowni	Zagrożenia dla sprzętu
Awaria zasilania	Skoki napięcia / przerwy w dostawie	Zagrożenia dla sprzętu
Awaria sprzętu	Awaria dysków, modułów, płyty głównej, sterowników, routerów	Zagrożenia dla sprzętu
Nieuprawniony dostęp	Nadane zbyt wysokie uprawnienia użytkownikom lub brak kontroli nad dostępem do plików, baz, komputerów	Zagrożenia dla danych
Kradzież tożsamości	Przejęcie poczty, np. gmailowej, pozyskanie danych z dowodu osobistego i w rezultacie no. założenie firmy „słupa”, wzięcie kredytu, zakup na allegro na cudze konto	Zagrożenia dla danych
Nieuprawniona modyfikacja / usunięcie	– może mieć również charakter niezamierzony lub być efektem pomyłki - sfałszowanie danych przez osoby z wewnątrz lub zewnątrz organizacji	Zagrożenia dla danych
Nieuprawnione kopiowanie danych	Kopiowanie danych z katalogów, dysków, baz, programów, kserowanie i robienie zdjęć przez pracownika lub przez osobę obcą	Zagrożenia dla danych
Kradzież danych lub nośników	Na zewnątrz i wewnątrz organizacji	Zagrożenia dla danych
Utrata / kradzież danych dostępowych	Haseł, kluczy, certyfikatów	Zagrożenia dla danych
Błąd / awaria	Uszkodzenie bazy danych, programu kadrowo-płacowego	Zagrożenia dla

oprogramowania		danych
Brak / błędy w wykonywaniu kopii bezpieczeństwa	Doraźne lub za rzadkie wykonywanie kopii, błędy podczas procesu wykonywania kopii, kopie dostępne w sieci bez zabezpieczeń	Zagrożenia dla danych
Udostępnianie danych osobom nieupoważnionym	Upublicznienie danych w przestrzeni publicznej, dostęp przez Internet, przesłanie lub wydawanie informacji osobie nieupoważnionej, wyrzucanie na śmietnik, wynoszenie na wolne powietrze	Zagrożenia dla danych
Nieprawidłowe / brak procedur niszczenia nośników z danymi –	Wyrzucenie uszkodzonych nośników bez ich zniszczenia, wyrzucenie niezniszczonych pendrive, DVD	Zagrożenia dla danych
Nieprawidłowe / brak procedur napraw w serwisach zewnętrznych	Naprawa sprzętu z nośnikami w serwisie bez standardu bezpiecznej naprawy i bez umowy bezpieczeństwa	Zagrożenia dla danych
Nieprzestrzeganie procedur	Świadome naruszenie pisemnych lub ustnych procedur, np. niewylogowywanie się z systemu, przekazywanie haseł koledze	Błędy ludzkie
Pomyłki administratorów, użytkowników	Pomyłkowe udostępnienie, wysłanie do złego odbiorcy, błędne zabezpieczenia	Błędy ludzkie
Brak świadomości / wiedzy	Braki w inteligencji, nieprzeszkolony personel	Błędy ludzkie
Błędy projektowe / konfiguracyjne	Błędy programistów prowadzące do niewłaściwego przetwarzania danych, niezabezpieczenie danych w bazie www przed indeksacją robotów google	Błędy ludzkie
Brak aktualnej dokumentacji	Brak instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania utrudnia przywracanie środowiska i zarządzanie nim gdy np. odejdzie pracownik IT	Zagrożenia ciągłości działania
Nieprawidłowe / brak umowy o współpracy	Brak odpowiedzialności stwarza ryzyko braku staranności	Zagrożenia ciągłości działania
Nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego	Umowy wymagają przedłużania, czas reakcji nie oznacza czasu naprawy	Zagrożenia ciągłości działania
Upadek firmy outsourcingowej lub dostawczej –	Ryzyko braku zastępstw, np. dla hostingodawcy poczty, dla wsparcia do zakupionej aplikacji	Zagrożenia ciągłości działania
Zagubienie nośnika danych	Na zewnątrz i wewnątrz organizacji	Zagrożenie dla danych
Awaria łączy telekomunikacyjnych –	Krytyczna w przypadku usług chmurowych oraz platform SaaS	Zagrożenia ciągłości działania

C. Analiza ryzyka przetwarzanych danych w SZKOLE PODSTAWOWEJ NR 1 WE WROCŁAWIU

Na następnych stronach dokonano szacowania ryzyka w obszarze przetwarzania danych osobowych. Szacowanie to ma formę tabelkową, co powinno ułatwić odczytanie i zrozumienie procesu analitycznego w tym zakresie.

Analizy dokonano dla każdego z procesów zidentyfikowanych w ramach Rejestru Czynności. W przypadku procesów z tej samej kategorii przyjęto analizę zbiorczą, jeżeli takie działanie było uzasadnione zastosowaniem w przetwarzaniu tych samych rozwiązań organizacyjnych, technicznych oraz obejmowało podobny zakres danych osobowych.

Elementem dokonanej analizy ryzyka jest Wstępna ocena skutków dla ochrony danych osobowych, której obowiązek przeprowadzenia wynika z art. 35 RODO. Obowiązek przeprowadzenia takiej oceny wynika jednoznacznie z Wytycznych Grupy Roboczej ds. art. 29 z dnia 4 października 2017 roku pt. „Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679".

Proces Wstępnej oceny ma na celu określenie, czy dla danego procesu podmiot powinien przeprowadzić pełną Ocenę Skutków dla Ochrony Danych, czyli szeroką i szczegółową analizę, której celem ma być określenie czy podmiot rzeczywiście może realizować dane działanie (czy nie narusza ono praw i wolności osób, których dane dotyczą) oraz jakie wzmożone środki bezpieczeństwa powinien przewidzieć dla takiego działania.

Wstępna ocena jest realizowana poprzez zadanie 10 pytań do każdego danego procesu. Jeżeli co najmniej 2 odpowiedzi na pytania są pozytywne to jest to przesłanka za uznaniem konieczności realizacji pełnej Oceny Skutków dla tego procesu. Te pytania to:

1) Czy w procesie realizowana jest ewaluacja lub ocena podmiotu danych, w tym profilowanie i przewidywanie (np. tworzenie profili zachowania lub profili marketingowych)?
2) Czy występuje zautomatyzowane podejmowanie decyzji wywołujące skutki prawne lub podobne istotne skutki wobec podmiotu danych? (np. przetwarzania mogące prowadzić do automatycznej blokady konta, usunięcia danych, odmówienia świadczenia usługi);
3) Czy występuje systematyczne monitorowanie podmiotów danych?
4) Czy przetwarzane są szczególne kategorie danych (np. dane zdrowotne, dane biometryczne)?
5) Czy dane są przetwarzane na dużą skalę? (bierzemy pod uwagę liczbę osób, których dane dotyczą, ilość danych, czas trwania oraz zakres geograficzny przetwarzania);
6) Czy dokonuje się porównania lub połączenia zestawów danych? (np. pochodzących z co najmniej dwóch operacji przetwarzania danych przeprowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą);
7) Czy przetwarzane są dane osobowe osób wymagających szczególnej opieki (np. dzieci)?
8) Czy występuje innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych? (np. połączenie technologii rozpoznającej czytanie maili, monitoring zachowania z analizą chat);
9) Czy występuje transgraniczne przekazywanie danych poza Europejski Obszar Gospodarczy?

10) Czy przetwarzanie samo w sobie „uniemożliwia” osobom, których dane dotyczą, wykorzystanie prawa lub korzystanie z usługi lub umowy? (np. sprawdzanie przez bank klientów w bazie informacji kredytowej, aby podjąć decyzję o zaproponowaniu im pożyczki lub nie).

W tym miejscu należy wskazać, że w ramach analizy ryzyka zanotowano jedynie ostateczną odpowiedź, czy dla danego procesu wymagana jest pełna Ocena Skutków dla Ochrony Danych, czy też nie, tj. czy dla danego procesu udzielono co najmniej dwóch pozytywnych odpowiedzi na dziesięć z powyższych pytań.

(analiza ryzyka na następnej stronie)

ANALIZA RYZYKA W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH - Szkoła Podstawowa nr 1 im. Marii Dąbrowskiej we Wrocławiu										
L.P.	Proces (liczba porządkowa z Rejestru Czynności)	Wrażliwość aktywa (dla organizacji/ w ujęciu społecznym)	Zagrożenia, co do których istnieją szczególne obawy ich wystąpienia w procesie	Potencjalne następstwa w przypadku zaistnienia określonych zagrożeń	Zastosowane środki kontroli i bezpieczeństwa	Szacowanie ryzyka - poufność	Szacowanie ryzyka - dostępność	Szacowanie ryzyka - integralność	Decyzja dot. stwierdzonego ryzyka - czy należy podejmować jakieś działania	** Wyniki Wstępnej Oceny Skutków dla Ochrony Danych - czy wymagane jest zrealizowanie dla procesu pełnej Oceny Skutków dla Ochrony Danych?
1	1,2	Niska	1.Błąd ludzki 2.Szkodliwe oprogramowanie (w odniesieniu do danych księgowych i bazodanowych) 3.Nieuczciwe działania 4.Nieprzestrzeganie procedur wewnętrznych	Uzyskanie dostępu do ograniczonej ilości danych przez ograniczoną liczbę osób nieuprawnionych	1. Szkolenia dla pracowników administracyjnych szkoły 2. Stosowanie dokumentu "Podstawowe reguły przetwarzania danych" przez pracowników administracyjnych 3. Posiadanie procedury działania na wypadek incydentu bezpieczeństwa 4. Przeprowadzanie okresowych audytów przez IODO	4	2	4	1. Zakaz wykorzystywania prywatnych narzędzi (laptopów, smartfonów) do pracy. 2. Weryfikacja przestrzegania powyższego działania 3. Sugerowane jest kształcenie pracowników administracyjnych pod kątem zasad postępowania oraz pod kątem możliwych zagrożeń dla bezpieczeństwa danych osobowych. Szkolenia tego typu w formacie prezentacji lub e-learning powinny odbywać się nie rzadziej niż raz na 1 rok.	Nie
2	3,4,5	Wysoka	1. Nieprzestrzeganie procedur wewnętrznych 2. Ataki socjotechniczne 3. Złośliwe oprogramowanie (wirusy, spyware) 4. Błąd ludzki	Uzyskanie dostępu do ograniczonej ilości danych przez ograniczoną ilość osób nieuprawnionych	1. Szkolenia dla pracowników administracyjnych 2. Stosowanie dokumentu "Podstawowe reguły przetwarzania danych" przez pracowników administracyjnych 3. Posiadanie procedury działania na wypadek incydentu bezpieczeństwa 4. Przeprowadzanie okresowych audytów przez IODO	3	2	3	1. Sugerowane jest kształcenie pracowników administracyjnych pod kątem zasad postępowania oraz pod kątem możliwych zagrożeń dla bezpieczeństwa danych osobowych. Szkolenia tego typu w formacie prezentacji lub e-learning powinny odbywać się nie rzadziej niż raz na 1 rok.	Nie

3	6,7,8,9,10, 11	Średnia/ Wysoka	1. Nieprzestrzeganie procedur wewnętrznych 2. Ataki socjotechniczne 3. Błąd ludzki 4. Złośliwe oprogramowanie (wirusy, spyware	1. Uzyskanie dostępu do ograniczonej ilości danych przez ograniczoną ilość osób nieuprawnionych 2. Zgubienie danych	1. Szkolenia dla pracowników administracyjnych 2. Stosowanie dokumentu "Podstawowe reguły przetwarzania danych" przez pracowników administracyjnych 3. Posiadanie procedury działania na wypadek incydentu bezpieczeństwa 4. Przeprowadzanie okresowych audytów przez IODO	3	2	3	1. Sugerowane jest kształcenie pracowników administracyjnych pod kątem zasad postępowania oraz pod kątem możliwych zagrożeń dla bezpieczeństwa danych osobowych. Szkolenia tego typu w formacie prezentacji lub e-learning powinny odbywać się nie rzadziej niż raz na 1 rok.	Nie
4	12,13,14,15, 16,17,18,19, 20, 21, 22	Wysoka	1. Nieprzestrzeganie procedur 2. Błąd ludzki 3.Złośliwe oprogramowanie 4.Ataki socjotechniczne 5.Nieuczciwe działanie	1. Uzyskanie dostępu do ograniczonej ilości danych przez ograniczoną ilość osób nieuprawnionych 2. Zagubienie danych.	1. Szkolenia dla pracowników administracyjnych 2. Stosowanie dokumentu "Podstawowe reguły przetwarzania danych" przez pracowników administracyjnych 3. Posiadanie procedury działania na wypadek incydentu bezpieczeństwa 4. Przeprowadzanie okresowych audytów przez IODO	5	4	1	1. Zakaz wykorzystywania prywatnych narzędzi (laptopów, smartfonów) do celów pracowniczych 2. Weryfikowanie przestrzegania powyższego działania 3. Sugerowane jest kształcenie pracowników administracyjnych pod kątem zasad postępowania oraz pod kątem możliwych zagrożeń dla bezpieczeństwa danych osobowych. Szkolenia tego typu w formacie prezentacji lub e-learning powinny odbywać się nie rzadziej niż raz na 1 rok	Nie
5	23,25,26,27	Średnia	1. Nieprzestrzeganie procedur wewnętrznych 2. Błąd ludzki 3. Ataki socjotechniczne 4. Złośliwe oprogramowanie 5. Ataki na infrastrukturę	1.Utrata dostępności do portali, 2. uzyskanie dostępu do ograniczonej ilości danych przez ograniczoną ilość osób nieuprawnionych	1. Szkolenia dla pracowników administracyjnych 2. Stosowanie dokumentu "Podstawowe reguły przetwarzania danych" przez pracowników administracyjnych 3. Posiadanie procedury działania na wypadek incydentu bezpieczeństwa 4. Przeprowadzanie okresowych audytów przez IODO 5. Ustalenie odpowiednio bezpiecznego hasła do logowania	5	3	1	1. Zakaz wykorzystywania prywatnych narzędzi (laptopów, smartfonów) do celów pracowniczych 2. Sugerowane jest kształcenie pracowników administracyjnych pod kątem zasad postępowania oraz pod kątem możliwych zagrożeń dla bezpieczeństwa danych osobowych. Szkolenia tego typu w formacie prezentacji lub e-learning powinny odbywać się nie rzadziej niż raz na 1 rok.	Nie

6	24, 28	Niskie	1.Błąd ludzki 2. Nieprzestrzeganie procedur 3.Nieuczciwe działania 4.Ataki socjotechniczne	Uzyskanie dostępu do ograniczonej ilości danych przez ograniczoną ilość osób nieuprawnionych	1. Szkolenia dla pracowników administracyjnych 2. Stosowanie dokumentu "Podstawowe reguły przetwarzania danych" przez pracowników administracyjnych 3. Posiadanie procedury działania na wypadek incydentu bezpieczeństwa 4. Przeprowadzanie okresowych audytów przez IODO	2	3	1	1. Sugerowane jest kształcenie pracowników administracyjnych pod kątem zasad postępowania oraz pod kątem możliwych zagrożeń dla bezpieczeństwa danych osobowych. Szkolenia tego typu w formacie prezentacji lub e-learning powinny odbywać się nie rzadziej niż raz na 1 rok.	Nie
7	29,32	Niskie	1. Nieprzestrzeganie wewnętrznych procedur 2. Nieuczciwe działania 3. Ataki socjotechniczne 4. Błąd ludzki 5. Złośliwe oprogramowanie (wirusy, spyware)	Uzyskanie dostępu do ograniczonej ilości danych przez ograniczoną ilość osób nieuprawnionych	1. Szkolenia dla pracowników administracyjnych 2. Stosowanie dokumentu "Podstawowe reguły przetwarzania danych" przez pracowników administracyjnych 3. Posiadanie procedury działania na wypadek incydentu bezpieczeństwa 4. Przeprowadzanie okresowych audytów przez IODO	2	1	2	Sugerowane jest kształcenie pracowników administracyjnych pod kątem zasad postępowania oraz pod kątem możliwych zagrożeń dla bezpieczeństwa danych osobowych. Szkolenia tego typu w formacie prezentacji lub e-learning powinny odbywać się nie rzadziej niż raz na 1 rok.	Nie
8	31	Wysoka	1. Ataki na infrastrukturę 2. Złośliwe oprogramowanie 3. Nieprzestrzeganie wewnętrznych procedur	Uzyskanie dostępu do danych dot. wizerunku wychowanków i pracowników oraz możliwość nieuprawnionego ujawnienia, utrata danych,	1.Ograniczenie dostępu do danych do ściśle ograniczonego kręgu osób w organizacji 2. Przeprowadzanie okresowych audytów przez IODO	3	2	3	Sugerowane jest kształcenie pracowników administracyjnych pod kątem zasad postępowania oraz pod kątem możliwych zagrożeń dla bezpieczeństwa danych osobowych. Szkolenia tego typu w formacie prezentacji lub e-learning powinny odbywać się nie rzadziej niż raz na 1 rok.	Są spełnione warunki dla OSOD, jednocześnie w tym obszarze znajduje zastosowanie art.. 35 ust. 10 RODO w zw. z art. 108a Prawa oświatowego. Odrębnie przeprowadzono konsultacje społeczne oraz analizę klauzuli interesu

										publicznego w ramach dokumentu 5a. Polityki Ochrony Danych Osobowych
9	30, 33, 34	Niska/ Średnia	1.Ataki socjotechniczne 2.Złośliwe oprogramowanie (wirusy, spyware)	Uzyskanie dostępu do ograniczonej ilości danych przez ograniczoną ilość osób nieuprawnionych	1. Szkolenia dla pracowników administracyjnych szkoły 2. Stosowanie dokumentu "Podstawowe reguły przetwarzania danych" przez pracowników administracyjnych 3. Posiadanie procedury działania na wypadek incydentu bezpieczeństwa 4. Przeprowadzanie okresowych audytów przez IODO	4	2	1	1. Zakaz wykorzystywania prywatnych narzędzi (laptopów, smartfonów) do pracy. 2. Sugerowane jest kształcenie pracowników administracyjnych pod kątem zasad postępowania oraz pod kątem możliwych zagrożeń dla bezpieczeństwa danych osobowych. Szkolenia tego typu w formacie prezentacji lub e-learning powinny odbywać się nie rzadziej niż raz na 1 rok.	Nie

ROZDZIAŁ IV:
OCENA ZASADNOŚCI PROCESÓW Z POWOŁANIEM NA KLAUZULĘ INTERESU PUBLICZNEGO LUB KLAUZULĘ WŁADZY PUBLICZNEJ (ART. 6 UST. 1 LIT. E RODO)

Zgodnie z motywem 45 preambuły RODO:

(45) Jeżeli przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego, któremu podlega administrator, lub jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, podstawę przetwarzania powinno stanowić prawo Unii lub prawo państwa członkowskiego. Niniejsze rozporządzenie nie nakłada wymogu, aby dla każdego indywidualnego przetwarzania istniało szczegółowe uregulowanie prawne. Wystarczyć może to, że dane uregulowanie prawne stanowi podstawę różnych operacji przetwarzania wynikających z obowiązku prawnego, któremu podlega administrator, lub że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Prawo Unii lub prawo państwa członkowskiego powinno określać także cel przetwarzania.

Jednocześnie zgodnie z art. 6 ust. 3 RODO

3. Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona:
a) w prawie Unii; lub
b) w prawie państwa członkowskiego, któremu podlega administrator.
Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) - musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. (…) Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

Nadto zgodnie z art. 21 ust. 1 RODO

Artykuł 21
Prawo do sprzeciwu
1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw - z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Z zestawienia powołanych regulacji wynika, że jednostki oświatowe w ramach swojej działalności mogą przetwarzać dane osobowe nie tylko w tych przypadkach, gdy przepisy powszechnie obowiązującego prawa wyraźnie na to zezwalają, ale również wówczas gdy prawo do takiego przetwarzania można jednoznacznie wyinterpretować z istniejących regulacji z powołaniem na klauzulę interesu publicznego. Jednocześnie przetwarzanie tego rodzaju nie powinno generalnie naruszać praw ani wolności osób, których dane dotyczą, chyba że administrator jest w stanie wykazać, że w danym przypadku interes publiczny przeważa nad określonymi prawami lub wolnościami osób fizycznych.

W ramach niniejszego dokumentu „Oceny Zasadności Procesów" Szkoła Podstawowa nr 1 im. Marii Dąbrowskiej we Wrocławiu dokonuje weryfikacji czy działania, które realizuje na danych osobowych z powołaniem na klauzulę interesu publicznego / władzy publicznej, są działaniami odpowiadającymi warunkom RODO.

W ramach Rejestru Czynności w Szkole Podstawowej zidentyfikowano następujące procesy, dla których przetwarzanie odbywa się z powołaniem na klauzulę interesu publicznego / władzy publicznej:

a) Monitoring wizyjny
b) Rejestr wejść/wyjść na teren Szkoły
c) Wywieszanie informacji na tablicach na terenie Szkoły Podstawowej
d) Zamieszczanie danych osobowych w gazetce szkolnej
e) Zamieszczanie danych osobowych na stronie www Szkoły Podstawowej
f) Wycieczki
g) Konkursy

Procesy te zostaną przeanalizowane odrębnie, zgodnie z przyjętą przez Szkołę Podstawową formułą pytań i odpowiedzi, których celem jest weryfikacja prawidłowości przyjętych przez Szkołę rozwiązań oraz ich zgodności z prawami i wolnościami osób fizycznych, których dane dotyczą.

A. **MONITORING WIZYJNY** – TEST KLAUZULI INTERESU PUBLICZNEGO

Jaki jest cel operacji przetwarzania

Zapewnienie bezpieczeństwa osób i mienia przebywających w placówce.

Jaka jest podstawa prawna dla operacji przetwarzania

Możliwość wprowadzenia monitoringu wizyjnego w Szkole Podstawowej została przewidziana w art. 108a ustawy – Prawo oświatowe. Przepis ten wszedł w życie z dniem 25 maja 2018 roku. Zgodnie z powołanym przepisem:

Art. 108a Prawa oświatowego

1. Jeżeli jest to niezbędne do zapewnienia bezpieczeństwa uczniów i pracowników lub ochrony mienia dyrektor szkoły lub placówki, w uzgodnieniu z organem prowadzącym szkołę lub placówkę oraz po przeprowadzeniu konsultacji z radą pedagogiczną, radą rodziców i samorządem uczniowskim, może wprowadzić szczególny nadzór nad pomieszczeniami szkoły lub placówki lub terenem wokół szkoły lub placówki w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring).
2. Monitoring nie powinien stanowić środka nadzoru nad jakością wykonywania pracy przez pracowników szkoły lub placówki.
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 sanitarnohigienicznych, 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. 1 i nie naruszy to godności oraz innych dóbr osobistych uczniów, pracowników i innych osób, w szczególności zostaną zastosowane techniki uniemożliwiające rozpoznanie przebywających w tych pomieszczeniach osób.
4. Nagrania obrazu zawierające dane osobowe uczniów, pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, szkoła lub placówka przetwarza wyłącznie do celów, dla których zostały zebrane, i przechowuje przez okres nie dłuższy niż 3 miesiące od dnia nagrania.
5. Po upływie okresu, o którym mowa w ust. 4, uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe uczniów, pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej.
6. Dyrektor szkoły lub placówki informuje uczniów i pracowników szkoły lub placówki o wprowadzeniu monitoringu, w sposób przyjęty w danej szkole lub placówce, nie później niż 14 dni przed uruchomieniem monitoringu.
7. Dyrektor szkoły lub placówki przed dopuszczeniem osoby do wykonywania obowiązków służbowych informuje ją na piśmie o stosowaniu monitoringu.
8. W przypadku wprowadzenia monitoringu dyrektor szkoły lub placówki oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż dzień przed jego uruchomieniem.
9. Dyrektor szkoły lub placówki uzgadnia z organem prowadzącym szkołę 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.

Jaki interes publiczny lub element władztwa publicznego będzie realizowany/wspierany przez to przetwarzanie?

Bezpieczeństwo Szkoły Podstawowej, ale przede wszystkim uczących się w placówce dzieci, jest w tym przypadku w interesie publicznym. Obecność monitoringu wizyjnego pełni realnie funkcję prewencyjną – osoby, które mogłyby chcieć porwać dziecko lub je skrzywdzić korzystając z jego obecności na terenie Szkoły Podstawowej, w większości wypadków zrezygnują z tego zamiaru, kiedy dostrzegą obecność monitoringu. Ten rodzaj zabezpieczenia, który zapewnia nagranie wizerunku sprawcy ewentualnego wykroczenia lub przestępstwa, które stanowi jednoznaczny dowód winy, pełni wystarczającą funkcję odstraszającą. Jednocześnie bezpieczeństwo dzieci na terenie Szkoły Podstawowej jest jednym z najważniejszych zadań jednostki.

Czy przetwarzanie jest niezbędne, aby osiągnąć jeden lub więcej konkretnych celów operacji przetwarzania?

Zapewnienie bezpieczeństwa dzieciom na terenie Szkoły Podstawowej można zapewnić na wiele różnych sposobów. Tym podstawowym jest uważny nadzór nauczycieli, wychowawców nad dziećmi w grupie. Jednocześnie człowiek bywa omylny, może być zmęczony i wsparcie ze strony systemów wizyjnych będzie stanowić właściwe uzupełnienie tej podstawowej metody zapewnienia bezpieczeństwa. Nadto system monitoringu działa również po godzinach pracy, co pozwala na zabezpieczenie dostępu do Szkoły Podstawowej, zabezpieczenie majątku również w okresie, gdy na miejscu nie ma żadnego pracownika.

Czy przyjęty sposób realizacji celu nie jest nadmierny?

Szkoła Podstawowa nie posiada informacji, aby przyjęty sposób realizacji celu był uznawany przez pracowników lub rodziców dzieci za intruzywny, niewygodny, nieprzyjemny, niepotrzebny. Systemy monitoringu obecnie są społecznie akceptowane, a nawet oczekiwane, z uwagi na funkcję bezpieczeństwa, które zapewniają.

Jednocześnie kamery monitoringu wizyjnego nie obejmują pomieszczeń intymnych (np. toalety), czy też pomieszczeń socjalnych.

Czy prawa i wolności osób, których dane dotyczą są wystarczająco chronione?

Nagrania z systemu monitoringu są wykorzystywane z zasady w przypadku wystąpienia naruszeń. Nagrania te nie służą do rozliczania pracowników lub rodziców z ich codziennych zachowań lub sposobu wykonywania pracy. Dodatkowo do nagrań z monitoringu ma dostęp ograniczony katalog osób w jednostce.

Tego rodzaju praktyka wydaje się stanowić odpowiednie zabezpieczenie interesów praw i wolności osób fizycznych.

Czy osoby, których dane dotyczą spodziewają się przetwarzania ich danych w omawianym zakresie?

Przy wejściu do Szkoły Podstawowej pojawia się informacja w formie znaku graficznego o monitoringu wizyjnym na terenie jednostki. Nadto na tablicy informacyjnej wewnątrz jednostki pojawia się informacja o zasadach przetwarzania danych związanych z monitoringiem. W ten sposób realizowana jest podstawowa zasada ochrony danych osobowych – zasada transparentności. Dzięki temu poszczególne osoby mają wiedzę i świadomość monitorowania obiektu Szkoły Podstawowej.

Czy osoby, których dane dotyczą mogą sprzeciwić się takiemu przetwarzaniu ich danych osobowych?

Realnie nie. Przeczyłoby to idei monitoringu wizyjnego, gdyby osoba uwieczniona w ramach danego zdarzenia mogła skutecznie zażądać usunięcia nagrania.

Jaki jest charakter przetwarzanych danych? Czy dane tego rodzaju podlegają specjalnej ochronie na gruncie RODO?

Przetwarzany jest wizerunek i zachowań. Nie są to dane podlegające szczególnej ochronie.

Jakie zabezpieczenia zastosowano?

Dostęp do nagrań z monitoringu wymaga fizycznego dostępu do urządzenia odczytującego nagrania oraz wymaga podania danych dostępowych.

Wynik analizy

Należy uznać, że monitoring wizyjny jest działaniem Szkoły Podstawowej nakierowanym na realizację zadania – w postaci zapewnienia bezpieczeństwa placówki i dzieci – w interesie publicznym. Sposób działania Szkoły Podstawowej w tym obszarze nie skutkuje naruszeniem praw i wolności osób, których dane dotyczą.

B. REJESTR WEJŚĆ/WYJŚĆ NA TEREN SZKOŁY – TEST KLAUZULI INTERESU PUBLICZNEGO

Jaki jest cel operacji przetwarzania

Zapewnienie bezpieczeństwa osób i mienia przebywających w placówce.

Jaka jest podstawa prawna dla operacji przetwarzania

Zgodnie z art. 1 pkt 14) Prawa oświatowego Szkoła Podstawowa jest odpowiedzialna za utrzymywanie bezpiecznych i higienicznych warunków nauki, wychowania i opieki. Ponadto zgodnie z art. 68 ust. 1 pkt 6 - Dyrektor szkoły lub placówki w szczególności: (…) 6) wykonuje zadania związane z zapewnieniem bezpieczeństwa uczniom i nauczycielom w czasie zajęć organizowanych przez szkołę lub placówkę.

Jaki interes publiczny lub element władztwa publicznego będzie realizowany/wspierany przez to przetwarzanie?

Bezpieczeństwo Szkoły Podstawowej, ale przede wszystkim uczących się w placówce dzieci, jest w tym przypadku w interesie publicznym. Obecność rejestru wejść/wyjść pełni:

a) funkcję prewencyjną – osoby, które mogłyby chcieć porwać dziecko lub je skrzywdzić korzystając z jego obecności na terenie Szkoły Podstawowej, w większości wypadków zrezygnują z tego zamiaru, jeżeli będą zobowiązane podać przy wejściu swoje dane osobowe;
b) informacyjną – w przypadku zaistnienia danego zdarzenia placówka będzie w stanie zidentyfikować sprawcę zajścia na potrzeby dalszych czynności.

Jednocześnie bezpieczeństwo dzieci na terenie Szkoły Podstawowej jest jednym z najważniejszych zadań jednostki.

Czy przetwarzanie jest niezbędne, aby osiągnąć jeden lub więcej konkretnych celów operacji przetwarzania?

Zapewnienie bezpieczeństwa dzieciom na terenie Szkoły Podstawowej można zapewnić na wiele różnych sposobów. Tym podstawowym jest uważny nadzór nauczycieli, wychowawców nad dziećmi w grupie. Jednocześnie człowiek bywa omylny, może być zmęczony i wsparcie ze strony procedur o charakterze organizacyjnym stanowi właściwe uzupełnienie tej podstawowej metody zapewnienia bezpieczeństwa.

Czy przyjęty sposób realizacji celu nie jest nadmierny?

Największym problemem stosowania rejestru wejść/wyjść jest organizacja wpisów w okresach wzmożonego ruchu, kiedy poszczególne klasy kończą zajęcia i dzieci są masowo odbierane przez rodziców i opiekunów. W takim przypadku mogą tworzyć się zatory, które nie są pozytywnie odbierane przez rodziców i opiekunów.

Jednocześnie finalnie takie rozwiązanie jest społecznie akceptowane z uwagi na istotną wartość dodaną takiego mechanizmu, który pozwala na zapewnienie bezpieczeństwa dzieci. Istotne jest przy tym, aby przy stosowaniu rejestru zapewnić:

A. niemożność podejrzenia poprzednich wpisów w rejestrze przez osobę wpisującą swoje dane;
B. rzetelność danych wpisywanych do rejestru – tam gdzie osoba odpowiedzialna w placówce za prowadzenie rejestru ma wątpliwości co do tożsamości osoby wpisującej się do rejestru ma prawo poprosić taką osobę o okazanie dowodu tożsamości.

Czy prawa i wolności osób, których dane dotyczą są wystarczająco chronione?

Rejestr wejść/wyjść jest dostępny w całości tylko dla pracowników Szkoły Podstawowej odpowiedzialnych za jej bezpieczeństwo (np. woźny/woźna). Rodzice/opiekunowie/goście wpisujący się do rejestru nie powinni widzieć wpisów pozostałych osób, co Szkoła zapewnia poprzez odpowiednie przesłonięcie poprzednich wpisów.

Dane zbierane w ramach rejestru nie są nadmierne, a Szkoła nie zbiera kserokopii dowodów tożsamości.

Czy osoby, których dane dotyczą spodziewają się przetwarzania ich danych w omawianym zakresie?

Stosowanie rejestru wejść/wyjść jest raczej standardową praktyką w obszarze funkcjonowania jednostek administracyjnych, jak również podmiotów wolnorynkowych. Większość osób spodziewa się stosowania tego rodzaju praktyk w instytucjach, do których uczęszczają. Brak stosowania tego rodzaju procedur wynika zazwyczaj z braku środków organizacyjnych – zaangażowanie ludzkie w prowadzenie rejestru.

Czy osoby, których dane dotyczą mogą sprzeciwić się takiemu przetwarzaniu ich danych osobowych?

Sprzeciw wobec przetwarzania danych w rejestrze wejść/wyjść uniemożliwia danej osobie wstęp na teren placówki. Realnie więc osoba, która chce wejść na teren placówki, np. w celu odebrania swojego dziecka, w celu widzenia się z nauczycielem, pracownikiem administracyjnym nie może odmówić wpisania się do rejestru, a po wpisaniu do tego rejestru nie może od razu skutecznie zażądać wykreślenia z tego rejestru.

Jaki jest charakter przetwarzanych danych? Czy dane tego rodzaju podlegają specjalnej ochronie na gruncie RODO?

Przetwarzane są dane identyfikacyjne. Nie są to dane podlegające szczególnej ochronie.

Jakie zabezpieczenia zastosowano?

Rejestr wejść/wyjść ma formę papierową, książkową. Jest dostępny na portierni, pod nadzorem woźnego/woźnej. Po godzinach pracy jest zamykany w szafie na klucz, tak jak pozostała dokumentacja zawierająca dane osobowe.

Wynik analizy

Należy uznać, że stosowanie rejestru wejść/wyjść jest działaniem Szkoły Podstawowej nakierowanym na realizację zadania – w postaci zapewnienia bezpieczeństwa placówki i dzieci – w interesie publicznym. Sposób działania Szkoły Podstawowej w tym obszarze nie skutkuje naruszeniem praw i wolności osób, których dane dotyczą.

C. WYWIESZANIE INFORMACJI NA TABLICACH W SZKOLE – TEST KLAUZULI INTERESU PUBLICZNEGO

Jaki jest cel operacji przetwarzania

Integracja społeczności lokalnej wokół Szkoły Podstawowej. Wspieranie rozwoju uczniów. Informowanie rodziców o najważniejszych wydarzeniach i faktach.

Jaka jest podstawa prawna dla operacji przetwarzania

Zadaniem jednostek oświatowych, zgodnie z art. 1 Prawa oświatowego jest m.in. wychowanie rozumiane jako wspieranie dziecka w rozwoju ku pełnej dojrzałości w sferze fizycznej, emocjonalnej, intelektualnej, duchowej i społecznej, wzmacniane i uzupełniane przez działania z zakresu profilaktyki problemów dzieci i młodzieży.
(art. 1 pkt 3 Prawa oświatowego)

Jaki interes publiczny lub element władztwa publicznego będzie realizowany/wspierany przez to przetwarzanie?

Szkoła Podstawowa stoi na stanowisku, że wywieszanie na tablicach informacyjnych m.in. zdjęć z życia Szkoły, z wycieczek, konkursów, podpisanych prac plastycznych, sprzyja rozwojowi dzieci i integracji lokalnej społeczności. Jest to dodatkowy nakład pracy ze strony zespołu Szkoły Podstawowej i poza uczniami i ich rodzicami/opiekunami, nie ma innych beneficjentów.

Czy przetwarzanie jest niezbędne, aby osiągnąć jeden lub więcej konkretnych celów operacji przetwarzania?

Wywieszanie zdjęć, prac artystycznych na tablicach jest stosunkowo tanim sposobem osiągania wysokich efektów w obszarze realizacji zadania.

Czy przyjęty sposób realizacji celu nie jest nadmierny?

Z obserwacji wynika, że dzieci, rodzice oraz opiekunowie prawni są zadowoleni z faktu, że określone zdjęcia, prace, informacje znajdują się na tablicach na terenie Szkoły Podstawowej. Jednocześnie w przypadku, gdyby jakiś rodzic lub opiekun prawny wyraził sprzeciw wobec tej formy realizacji zadania przez Szkołę Podstawową, w takim przypadku Szkoła Podstawowa będzie pilnować, aby dane tego rodzica/opiekuna oraz jego dziecka nie podlegały tej formie przetwarzania.

Czy prawa i wolności osób, których dane dotyczą są wystarczająco chronione?

Dostęp do tablic informacyjnych będzie dostępny wyłącznie w budynku Szkoły Podstawowej, a więc będzie ograniczony do wąskiego kręgu zainteresowanych osób, które przynależą do jednej

społeczności. Należy uznać, że w tym przypadku i kontekście społecznych dane osobowe nie są narażone na niebezpieczeństwo.

Czy osoby, których dane dotyczą spodziewają się przetwarzania ich danych w omawianym zakresie?

Osoby, których dane dotyczą wiedzą, że tego rodzaju działania są prowadzone.

Czy osoby, których dane dotyczą mogą sprzeciwić się takiemu przetwarzaniu ich danych osobowych?

Tak. W przypadku sprzeciwu Szkoła Podstawowa zdejmie dane zdjęcia, prace lub informacje dotyczące tej osoby lub jej dziecka i nie będzie już wywieszać danych osobowych tej osoby oraz jej dziecka.

Jaki jest charakter przetwarzanych danych? Czy dane tego rodzaju podlegają specjalnej ochronie na gruncie RODO?

Są to dane dot. wizerunku oraz aktywności na zdjęcia, imię, nazwisko, prace artystyczne. Nie występują dane podlegające szczególnej ochronie.

Jakie zabezpieczenia zastosowano?

Dane osobowe są dostępnej wyłącznie wewnątrz budynku Szkoły Podstawowej, który jest zamykany na klucz oraz jest objęty monitoringiem wizyjnym.

Wynik analizy

Należy uznać, że wywieszanie na tablicach informacyjnych danych osobowych dot. dzieci oraz ich rodziców lub opiekunów prawnych jest zgodne z interesem publicznym i nie narusza praw lub wolności osób fizycznych, których dane dotyczą.

D. ZAMIESZCZANIE INFORMACJI W GAZETCE SZKOLNEJ – TEST KLAUZULI INTERESU PUBLICZNEGO

Jaki jest cel operacji przetwarzania

Integracja społeczności lokalnej wokół Szkoły Podstawowej. Wspieranie rozwoju dzieci. Informowanie rodziców o najważniejszych wydarzeniach i faktach.

Jaka jest podstawa prawna dla operacji przetwarzania

Zadaniem jednostek oświatowych, zgodnie z art. 1 Prawa oświatowego jest m.in. wychowanie rozumiane jako wspieranie dziecka w rozwoju ku pełnej dojrzałości w sferze fizycznej, emocjonalnej, intelektualnej, duchowej i społecznej, wzmacniane i uzupełniane przez działania z zakresu profilaktyki problemów dzieci i młodzieży.
(art. 1 pkt 3 Prawa oświatowego)

Wydawanie gazetki szkolnej wiąże się z informowaniem Rodziców dzieci nauczycieli o bieżących wydarzeniach z życia Szkoły Podstawowej. Ma ona charakter przede wszystkim integracyjny oraz wzmacniający samoocenę dziecka który widząc również samodzielnie siebie w czymś takim jak gazetka traktuje siebie jako członka szerszej społeczności, w której podejmuje określone role i funkcje. Gazetka pełni również funkcję informacyjną i edukacyjną z korzyścią dla rodziców, dzieci i nauczycieli. Tym samym wydawanie gazetki spełnia warunki dla uznania, iż jest to działanie wykonywane w ramach zadania nałożonego na Szkołę Podstawową przez przepisy prawa oświatowego.

Jaki interes publiczny lub element władztwa publicznego będzie realizowany/wspierany przez to przetwarzanie?

Rozwój dziecka, integracja społeczności, funkcje edukacyjne oraz informacyjne.

Czy przetwarzanie jest niezbędne, aby osiągnąć jeden lub więcej konkretnych celów operacji przetwarzania?

Przetwarzanie nie jest niezbędne i konieczne dla osiągnięcia celów operacji przetwarzania, w tym znaczeniu, że istnieją Szkoły Podstawowej, gdzie gazetki nie są wydawane, a realizują prawidłowo swoją misję edukacyjną. Jednocześnie Szkoła Podstawowa stoi na stanowisku, że wydawanie gazetki jest doskonałą formą wspierania misji edukacyjnej Szkoły Podstawowej. Stanowi niepowtarzalny sposób aktywizacji dzieci, nauczycieli, rodziców do wspólnej pracy i zabawy oraz pomaga poczuć się częścią społeczności.

Czy przyjęty sposób realizacji celu nie jest nadmierny?

Gazetki szkolne są narzędziem stosowanym w oświacie od kilkudziesięciu lat i do tej pory były społecznie powszechnie akceptowane. Nie można wszakże wykluczyć sytuacji, gdzie określona osoba będzie chciała wyrazić sprzeciw wobec przetwarzanie jej danych lub danych jej dziecka polegającego na publikacji określonych danych osobowych w gazetce. Szkoła Podstawowa bezwzględnie musi być wrażliwa na tego rodzaju wskazania i powinna umożliwiać wyrażanie sprzeciwu wobec przetwarzania danych osobowych. Należy zauważyć że wydawanie gazetki jest elementem funkcjonowania Szkoły Podstawowej, o którym każdy z rodziców i dzieci wie i nie jest to element zaskakujący dla osób, których dane dotyczą.

W przypadku gdyby gazetka miała zostać opublikowana przez Szkołę Podstawową powszechnie w sieci Internet w sposób umożliwiający dostęp do niej każdej osobie zainteresowanej przyjęto regułę, że Szkoła Podstawowa powinna odebrać zgodę na przetwarzanie danych na potrzeby gazetki od każdej osoby której dane osobowe są dostępne w gazetce (w tym wizerunek dane identyfikacyjne).

Mając na uwadze powyższe środki, których celem jest zbilansowanie praw stron, tj. środki informacyjne, swobodne umożliwienie wyrażenia sprzeciwu wobec przetwarzania danych, obowiązek uzyskania zgody w razie publikacji gazetki, należy uznać, że zastosowany środek jest proporcjonalny do celu i nie jest nadmierny.

Czy prawa i wolności osób, których dane dotyczą są wystarczająco chronione?

Tak. Dane osobowe zawarte w treści gazetki co do zasady są dostępne wyłącznie dla rodziców, nauczycieli, dzieci, ewentualnie ich grona najbliższych. Z kolei w przypadku, gdyby gazetka miała zostać opublikowana przez Szkołę Podstawową - tego rodzaju działanie wymaga uzyskania uprzedniej zgody osób zainteresowanych, mając na uwadze że z chwilą publikacji danych treści w sieci Internet Szkoła Podstawowa utraci nad nimi kontrolę.

Czy osoby, których dane dotyczą spodziewają się przetwarzania ich danych w omawianym zakresie?

Osoby, których dane dotyczą wiedzą, że tego rodzaju działania są prowadzone.

Czy osoby, których dane dotyczą mogą sprzeciwić się takiemu przetwarzaniu ich danych osobowych?

Tak. W przypadku sprzeciwu Szkoła Podstawowa nie będzie już więcej zawierać w treściach gazetki danych osobowych osób które wyraziły sprzeciw wobec przetwarzania ich danych w tym celu. Jednocześnie taki sprzeciw będzie mógł odnieść skutek wyłącznie w stosunku do przyszłych wydań gazetki, a to w związku z faktem, że Szkoła Podstawowa nie jest w stanie cofnąć dystrybucji, która została już zrealizowana.

Jaki jest charakter przetwarzanych danych? Czy dane tego rodzaju podlegają specjalnej ochronie na gruncie RODO?

Są to dane dot. wizerunku oraz aktywności na zdjęcia, imię, nazwisko, prace artystyczne. Nie występują dane podlegające szczególnej ochronie.

Jakie zabezpieczenia zastosowano?

Gazetka podlega dystrybucji w społeczności lokalnej więc w tym przypadku poziom zabezpieczeń nie obejmuje tych osób. Z kolei dane zawarte w gazety są zabezpieczone przed powszechnie dostępnym poprzez standardowe zabezpieczenie komputerów, na których realizowana jest gazetka, przed swobodnym dostępem osób z zewnątrz.

Wynik analizy

Należy uznać, że prowadzenie przez Szkołę Podstawową gazetki zawierającej dane osobowe dzieci oraz ich rodziców lub opiekunów prawnych jest zgodne z interesem publicznym. Jednocześnie w celu ochrony praw i wolności osób, których dane dotyczą konieczna jest pełna transparentność działania w obszarze wydawania gazetki, danie uprawnionym realnej możliwości wyrażenia sprzeciwu wobec tej formy przetwarzania, a w przypadku chęci powszechnej publikacji gazetki w sieci Internet, konieczne jest uprzednie zebranie zgody od osób, których dane dotyczą.

E. ZAMIESZCZANIE DANYCH OSOBOWYCH NA STRONIE WWW SZKOŁY PODSTAWOWEJ – TEST KLAUZULI INTERESU PUBLICZNEGO

Jaki jest cel operacji przetwarzania

Integracja społeczności lokalnej wokół Szkoły Podstawowej. Informowanie rodziców o danych identyfikacyjnych, doświadczeniu oraz wizerunkach nauczycieli zaangażowanych w pracę Szkoły Podstawowej, o dyżurach, prowadzonych zajęciach dodatkowych.

Niniejsze opracowanie nie dotyczy zamieszczania na stronie internetowej zdjęć z wizerunkami dzieci lub rodziców, dla których to działań w placówce przyjęto za podstawę przetwarzania zgodę, a nie klauzulę interesu publicznego.

Jaka jest podstawa prawna dla operacji przetwarzania

Zadaniem jednostek oświatowych, zgodnie z art. 1 Prawa oświatowego jest m.in.:

- realizacja prawa każdego obywatela Rzeczypospolitej Polskiej do kształcenia się oraz prawa dzieci i młodzieży do wychowania i opieki, odpowiednich do wieku i osiągniętego rozwoju
- wychowanie rozumiane jako wspieranie dziecka w rozwoju ku pełnej dojrzałości w sferze fizycznej, emocjonalnej, intelektualnej, duchowej i społecznej, wzmacniane i uzupełniane przez działania z zakresu profilaktyki problemów dzieci i młodzieży.

(art. 1 pkt 1 i 3 Prawa oświatowego)

Publikowanie informacji o kadrze zaangażowanej w świadczenie usług wychowawczo opiekuńczych w Szkole Podstawowej oraz o zasadach tego kształcenia ma istotne znaczenie dla realizacji zadań stawianych przed Szkołą Podstawową. Dzięki temu rodzice są w stanie zidentyfikować osoby odpowiedzialne za opiekę nad ich dziećmi, uzyskać bezpośredni kontakt do nich oraz przeczytać ważne dla siebie informacje. Taka transparentność buduje zaufanie pomiędzy kadrą Szkoły Podstawowej, co bezsprzecznie sprzyja lepszemu realizowaniu zadań określonych w art. 1 pkt 1 i pkt 3 Prawa oświatowego.

Jaki interes publiczny lub element władztwa publicznego będzie realizowany/wspierany przez to przetwarzanie?

Integracja społeczności i budowa zaufania w relacji Szkoła Podstawowa - rodzice/opiekunowie prawni.

Czy przetwarzanie jest niezbędne, aby osiągnąć jeden lub więcej konkretnych celów operacji przetwarzania?

Publikacja danych kadry jest jednym z elementów procesu budowania relacji w społeczności Szkoły Podstawowej. Trudno byłoby ten element zastąpić jakimkolwiek innym.

Czy przyjęty sposób realizacji celu nie jest nadmierny?

Powszechnie przyjętą praktyką jest publikowanie wizerunku i podstawowych danych osobowych członków kadry na stronie internetowej jednostki. Dane opublikowane na stronie obejmują wyłącznie dane związane z wykonywanym zawodem oraz te spośród informacji osobistych, które dany pracownik sam decyduje się podać, którymi chciałby się pochwalić (na przykład zainteresowania, ukończone kursy). Nie są publikowane informacje mające charakter osobisty, wrażliwy, nadmierny w stosunku do celu.

Czy prawa i wolności osób, których dane dotyczą są wystarczająco chronione?

Tak. Dane osobowe zawarte na stronie internetowej nie zawierają danych wrażliwych. Jednocześnie każdemu pracownikowi Szkoły Podstawowej przysługuje prawo do zgłoszenia sprzeciwu wobec takiej formy przetwarzania jego danych osobowych.

Czy osoby, których dane dotyczą spodziewają się przetwarzania ich danych w omawianym zakresie?

Osoby, których dane dotyczą wiedzą, że tego rodzaju działania są prowadzone. Szkoła Podstawowa zawiera stosowną klauzulę informacyjną już na etapie rekrutacji.

Czy osoby, których dane dotyczą mogą sprzeciwić się takiemu przetwarzaniu ich danych osobowych?

Tak. W przypadku sprzeciwu Szkoła Podstawowa nie będzie już więcej zamieszczać na stronie internetowej danych osobowych, co do których pracownik Szkoły Podstawowej wyraził swój sprzeciw, chyba że interes realizowany w danym przypadku przez Szkołę Podstawową będzie przeważał nad prawami i wolnościami pracownika Szkoły Podstawowej (np. informacje o zwolnieniu pracownika, tak aby rodzice wiedzieli, że jest to już osoba spoza grona pedagogicznego).

Jaki jest charakter przetwarzanych danych? Czy dane tego rodzaju podlegają specjalnej ochronie na gruncie RODO?

Są to dane identyfikacyjne, informacje o posiadanym wykształceniu i doświadczeniu, wizerunek, terminy dyżurów, prowadzone zajęcia dodatkowe. Nie występują dane podlegające szczególnej ochronie.

Jakie zabezpieczenia zastosowano?

Dane są publicznie dostępne na stronie internetowej w związku z czym dane nie podlegają szczególnym zabezpieczeniom.

Wynik analizy

Należy uznać, że zamieszczanie przez Szkołę Podstawową na stronie internetowej danych osobowych członków kadry Szkoły Podstawowej jest działaniem w interesie publicznym, w szczególności działaniem w interesie dzieci, które uczęszczają do Szkoły Podstawowej oraz ich rodziców. Jednocześnie w celu ochrony praw i wolności osób, których dane dotyczą konieczna jest pełna transparentność działania w obszarze publikowania danych na stronie oraz danie uprawnionym realnej możliwości wyrażenia sprzeciwu wobec tej formy przetwarzania.

F. ORGANIZACJA WYCIECZEK SZKOLNYCH

Jaki jest cel operacji przetwarzania

Rozwój psychofizyczny dzieci, które poprzez obcowanie z otaczającym światem w czasie wycieczki poznają kulturę, historię, rozbudzają zainteresowanie nauką, pobudzają empatię i inne.

Jaka jest podstawa prawna dla operacji przetwarzania

Zadaniem jednostek oświatowych, zgodnie z art. 1 Prawa oświatowego jest m.in. wychowanie rozumiane jako wspieranie dziecka w rozwoju ku pełnej dojrzałości w sferze fizycznej, emocjonalnej, intelektualnej, duchowej i społecznej, wzmacniane i uzupełniane przez działania z zakresu profilaktyki problemów dzieci i młodzieży.
(art. 1 pkt 3 Prawa oświatowego)

Jaki interes publiczny lub element władztwa publicznego będzie realizowany/wspierany przez to przetwarzanie?

Wychowanie i rozwój uczniów.

Czy przetwarzanie jest niezbędne, aby osiągnąć jeden lub więcej konkretnych celów operacji przetwarzania?

Dzieci na wycieczce biorą udział w wydarzeniach, imprezach lokalnych i ponadlokalnych, mają możliwość odwiedzenia miejsc, obejrzenia rzeczy, które pozwalają im spojrzeć szerzej na świat. Jest to efekt, którego nie da się osiągnąć, gdyby dzieci przebywały tylko na terenie Szkoły Podstawowej.

Czy przyjęty sposób realizacji celu nie jest nadmierny?

Wycieczka jest naturalnym elementem funkcjonowania Szkoły Podstawowej. Jednocześnie nie znajduje ona swojej jednoznacznej podstawy prawnej w przepisach prawa oświatowego i ustawy o systemie oświaty. Dlatego przetwarzanie danych i udostępnianie danych w celu organizacji wycieczki za podstawę prawną ma interes publiczny. Działania na danych osobowych w tym obszarze trudno uznać za nadmierne w stosunku do celu, który jest realizowany.

Czy prawa i wolności osób, których dane dotyczą są wystarczająco chronione?

Tak. Szkoła Podstawowa udostępnia dane wyłącznie w niezbędnym zakresie i tylko zaufanym dostawcom usług i świadczeń, które są realizowane w czasie wycieczki (na przykład transport, wizyta w muzeum, w kinie, ubezpieczenie).

Czy osoby, których dane dotyczą spodziewają się przetwarzania ich danych w omawianym zakresie?

Tak. Wycieczki są naturalnym elementem funkcjonowania Szkoły Podstawowej. O możliwości udostępnienia danych dzieci zewnętrznych dostawcom usług w związku z wycieczką rodzice/opiekunowie prawni są informowania w ramach klauzuli informacyjnej przy przyjmowaniu dziecka do Szkoły Podstawowej.

Czy osoby, których dane dotyczą mogą sprzeciwić się takiemu przetwarzaniu ich danych osobowych?

Rodzic może sprzeciwić się udziałowi dziecka w wycieczce.

Jaki jest charakter przetwarzanych danych? Czy dane tego rodzaju podlegają specjalnej ochronie na gruncie RODO?

Są to dane identyfikacyjne.

Jakie zabezpieczenia zastosowano?

Udostępnienie danych dostawcom usług i świadczeń związanych z wycieczką odbywa się zazwyczaj pocztą elektroniczną. Przyjęto regułę przesyłania plików z danymi osobowymi protokołem szyfrowanym, a w jego braku, plikiem zabezpieczonym odpowiednio złożonym lub długim hasłem.

Wynik analizy

Należy uznać, że przetwarzanie danych osobowych dzieci w celu realizacji wycieczki jest uprawnione w ramach interesu publicznego realizowanego przez Szkołę Podstawową.

G. ORGANIZACJA I UDZIAŁ W KONKURSACH (SZKOLNYCH I MIĘDZYSZKOLNYCH) – TEST KLAUZULI INTERESU PUBLICZNEGO

Jaki jest cel operacji przetwarzania

Przygotowanie dzieci do życia w społeczeństwie, rozwój współzawodnictwa.

Jaka jest podstawa prawna dla operacji przetwarzania

Zadaniem jednostek oświatowych, zgodnie z art. 1 Prawa oświatowego jest m.in. wychowanie rozumiane jako wspieranie dziecka w rozwoju ku pełnej dojrzałości w sferze fizycznej, emocjonalnej, intelektualnej, duchowej i społecznej, wzmacniane i uzupełniane przez działania z zakresu profilaktyki problemów dzieci i młodzieży.
(art. 1 pkt 3 Prawa oświatowego)

Jaki interes publiczny lub element władztwa publicznego będzie realizowany/wspierany przez to przetwarzanie?

Wychowanie i rozwój uczniów.

Czy przetwarzanie jest niezbędne, aby osiągnąć jeden lub więcej konkretnych celów operacji przetwarzania?

Konkursy, współzawodnictwo są elementem naturalnie występującym w życiu Szkoły Podstawowej. Trudno byłoby sobie wyobrazić inne działania, które efektywnie prowadziłyby do osiągnięcia tego samego celu.

Czy przyjęty sposób realizacji celu nie jest nadmierny?

Działania na danych osobowych w celu organizacji i przeprowadzenia konkursu nie są nadmierne. Przetwarzane są tylko dane identyfikacyjne oraz te dane, które wiążą się bezpośrednio z przedmiotem konkursu.

Czy prawa i wolności osób, których dane dotyczą są wystarczająco chronione?

Co do zasady tak. W toku organizacji konkursu przez cały czas dane dzieci podlegają takiej samej ochronie, jak na co dzień. W przypadku laureatów ich imiona, nazwiska, informacje o Szkole Podstawowej mogą zostać wyczytane publicznie. Jest to forma publikacji danych osobowych dziecka, ale z uwagi na ich bardzo ograniczony charakter z jednej strony, a z drugiej okoliczność, że tego rodzaju odczytanie ma istotne znaczenie kształtujące postawy prospołeczne, chęć zdrowej rywalizacji, należy uznać że nie dochodzi do naruszenia praw i wolności osób, których dane dotyczą.

Czy osoby, których dane dotyczą spodziewają się przetwarzania ich danych w omawianym zakresie?

Tak. Konkursy są naturalnym elementem funkcjonowania Szkoły Podstawowej. O możliwości udostępnienia danych dzieci innym podmiotom, w tym szkołom, w związku z konkursem rodzice/opiekunowie prawni są informowania w ramach klauzuli informacyjnej przy przyjmowaniu dziecka do Szkoły Podstawowej.

Jednocześnie, z drugiej strony można argumentować, że w przypadku konkursów międzyszkolnych organizowanych przez Szkołę, w których dochodzi do pozyskiwania przez Szkołę danych osobowych innych dzieci (z innych Szkół), przetwarzanie danych osobowych poszczególnych uczniów z powołaniem na klauzulę interesu publicznego może stanowić zbytnią ingerencję w obszar władzy rodzicielskiej. Dlatego w Szkole przyjęto regułę, zgodnie z którą w przypadku konkursów, dla których organizatorem jest Szkoła Podstawowa nr 1 im. Marii Dąbrowskiej we Wrocławiu wymagane jest uzyskanie zgody rodzica / opiekuna prawnego na udział ucznia w konkursie.

Czy osoby, których dane dotyczą mogą sprzeciwić się takiemu przetwarzaniu ich danych osobowych?

Rodzic / opiekun prawny może sprzeciwić się udziałowi dziecka w konkursie.

Jaki jest charakter przetwarzanych danych? Czy dane tego rodzaju podlegają specjalnej ochronie na gruncie RODO?

Są to dane identyfikacyjne oraz informacje związane z udziałem w konkursie oraz informacje o wyniku.

Jakie zabezpieczenia zastosowano?

Udostępnienie danych innym szkołom lub organizacjom odpowiedzialnym za przeprowadzenie konkursu odbywa się zazwyczaj pocztą elektroniczną. Przyjęto w Szkole Podstawowej regułę przesyłania plików z danymi osobowymi protokołem szyfrowanym, a w jego braku, plikiem zabezpieczonym odpowiednio złożonym lub długim hasłem.

Wynik analizy

Należy uznać, że przetwarzanie danych osobowych uczniów w celu realizacji lub udziału w konkursie jest uprawnione w ramach interesu publicznego realizowanego przez Szkołę Podstawową.

ROZDZIAŁ V:
PODSUMOWANIE

Zawarty w niniejszym dokumencie opis struktury Szkoły oraz występujących w Szkole procesów przetwarzania danych osobowych stanowi przejaw udokumentowania czynności audytu oraz analizy procesów przetwarzania danych osobowych występujących w placówce. W ramach Polityki dokonano wymaganej przez RODO ogólnej analizy ryzyka działalności placówki oraz dokonano analizy zgodności poszczególnych działań Szkoły z prawem ochrony danych osobowych (unijnym oraz krajowym).

Jednocześnie na pełną dokumentację ochrony danych osobowych w Szkole składają się dodatkowo:

1. Rejestr Czynności przetwarzania danych osobowych (Załącznik nr 1)
2. Wzory upoważnień dla pracowników i współpracowników Szkoły (Załącznik nr 2)
3. Instrukcje ochrony danych osobowych dla pracowników (Załącznik nr 3)
4. Procedura na wypadek kontroli ze strony Prezesa Urzędu Ochrony Danych Osobowych (Załącznik nr 4)
5. Wzory klauzul informacyjnych do stosowania przez Szkołę w bieżącej działalności (Załącznik nr 5)
6. Wzory klauzul zgody do stosowania przez Szkołę (Załącznik nr 6)
7. Wzory umów powierzenia przetwarzania danych osobowych (Załącznik nr 7)
8. Wzór umowy udostępnienia danych (Załącznik nr 8)
9. Wzór dokumentacji do organizacji konkursu przez Szkołę (Załącznik nr 9).

Tytułem objaśnienia:

1. Rejestr czynności – jest dokumentem wewnętrznym, sporządzonym w wykonaniu zobowiązania, o którym mowa w art. 30 ust. 1 i ust. 2 RODO. Jego celem jest zidentyfikowanie procesów zachodzących w Szkole oraz ich opisanie. Dokument ten wymaga okresowej weryfikacji i aktualizacji, w przypadku gdyby w Szkole miały pojawić się nowe procesy.

2. Wzory upoważnień – są elementem organizacyjnego systemu bezpieczeństwa danych przetwarzanych w Szkole. Każdy pracownik lub współpracownik Szkoły mający dostęp do danych powinien posiadać stosowane upoważnienie, do przetwarzania tych danych. Elementem upoważnienia jest zobowiązanie upoważnionego do zachowania w pełnej poufności danych, do których otrzymał dostęp. Upoważnienia opracowano na podstawie Rejestru Czynności, z uwzględnieniem struktury organizacyjnej Szkoły.
   Upoważnień nie daje się do podpisu podwykonawcom, którzy są osobami/podmiotami zewnętrznymi w stosunku do Szkoły (np. dostawca oprogramowania, podmiot archiwizujący dokumentację).

3. Instrukcja ochrony danych osobowych dla pracowników oraz Procedura na wypadek kontroli ze strony PUODO - są to dokumenty, które powinny zostać przedstawione wszystkim

pracownikom i współpracownikom, którzy uzyskują upoważnienie do przetwarzania danych osobowych w Szkole. Dokumenty te zawierają kluczowe informacje dot. reguł przetwarzania danych osobowych w ramach ich codziennej pracy.

4. Wzory klauzul informacyjnych – dokumenty zawierające treści informacyjne wymagane przez art. 13 i 14 RODO dla poszczególnych procesów zidentyfikowanych jako stale występujących w bieżącej działalności Szkoły. Dla procesów wpadkowych, konieczne jest opracowywanie odrębnych klauzul informacyjnych dostosowanych do danego przypadku.

5. Wzory klauzul zgody – dokumenty, którymi Szkoła powinna się posługiwać zbierając poszczególne zgody od uczniów lub ich rodziców/przedstawicieli prawnych.

6. Wzory umów powierzenia przetwarzania danych osobowych – są to wzory umów przygotowane z uwzględnieniem warunków wynikających z art. 28 RODO. Powinny one zastąpić umowy, które do tej pory (przed wejściem do stosowania RODO) funkcjonowały w oparciu o art. 31 ustawy o ochronie danych osobowych (z 1997 roku). W załącznikach ujęto ogólne wzory umów, jak również wzory umów dostosowane do najczęściej występujących w praktyce Szkoły przypadków.

7. Wzór umowy udostępnienia danych – ten wzór będzie znajdował rzadko zastosowanie w praktyce działalności Szkoły. Dotyczy to tych wszystkich przypadków, gdy Szkoła jako administrator danych, zgodnie z prawem, przekazuje na własność poszczególne dane osobowe innemu podmiotowi (i to nie w celu wykonania zobowiązania wynikającego z przepisu prawa). Taka umowa powinna być podpisana np. w przypadku podjęcia współpracy z ośrodkiem medycznym, któremu Szkoła chce przekazać dane osobowe uczniów, których rodzice wyrazili zgodę na udział uczniów w dodatkowych badaniach (np. słuchu, wzroku, skóry).

8. Wzór dokumentacji do organizacji konkursu – te wzory dotyczą wyłącznie tych przypadków, gdy Szkoła organizuje konkurs o charakterze międzyszkolnym. Dla pozostałych przypadków Szkoła nie musi posiadać odrębnych wzorów (tj. dla konkursu wewnątrzszkolnego nie ma potrzeby uzyskiwania żadnych odrębnych zgód, a w konkursie organizowanym przez inną szkołę/podmiot, to ta szkoła/podmiot powinna przedstawić swoje klauzule do stosowania).

Działając w imieniu Szkoły Podstawowej nr 1 im. Marii Dąbrowskiej we Wrocławiu z dniem 19.11.2018 r. przyjmuję niniejszą Politykę Ochrony Danych Osobowych do stosowania wraz ze wszystkimi Załącznikami.

_____

Dyrektor Szkoły Podstawowej nr 1 we Wrocławiu