Szkoła Podstawowa im. Marii Skłodowskiej-Curie w Starych Bielicach

Polityka ochrony danych osobowych

Zatwierdzam do stosowania

…….
Data i podpis

Niniejszy dokument jest Polityką Ochrony Danych Osobowych w rozumieniu RODO – Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz. Urz. UE L 119, s.1).

Zawiera on:

a) opis zasad ochrony danych obowiązujących w Szkole Podstawowej im. Marii Skłodowskiej-Curie w Starych Bielicach
b) odwołania do procedur i instrukcji dotyczących poszczególnych obszarów ochrony danych osobowych.

Polityka Ochrony Danych Osobowych została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymaganiami RODO.

Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Dyrektor Szkoły Podstawowej im. Marii Skłodowskiej-Curie w Starych Bielicach. Za nadzór i monitorowanie przestrzegania Polityki odpowiada Inspektor Ochrony Danych (IOD). Do stosowania Polityki zobowiązani są przetwarzający dane osobowe.

§ 1 Skróty i definicje

Stosowane w niniejszym dokumencie skróty i definicje oznaczają:

a) Polityka oznacza niniejszą Politykę bezpieczeństwa, o ile co innego nie wynika wyraźnie z kontekstu,
b) RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1),
c) Dane osobowe oznaczają wszystkie informacje dotyczące zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie takiego identyfikatora jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
d) Dane szczególnych kategorii oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej,
e) Osoba oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu,
f) Podmiot przetwarzający oznacza organizację lub osobę, której Administrator powierzył przetwarzanie danych osobowych (np. usługodawca IT),
g) Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się,
h) Eksport danych oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej,
i) RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych,

j) Administrator Danych oznacza Szkołę Podstawową im. Marii Skłodowskiej-Curie w Starych Bielicach, reprezentowaną przez Dyrektora.

§ 2 Inspektor Ochrony Danych

1. Administrator Danych jest podmiotem publicznym, który na mocy art. 37 ust. 1 RODO ma obowiązek powołania Inspektora Ochrony Danych (IOD).
2. Osoba powołana na stanowisko IOD posiada:
    a) odpowiednią wiedzę fachową tj. gruntowną wiedzę na temat krajowego i europejskiego prawa oraz praktyk w dziedzinie ochrony danych osobowych,
    b) znajomość struktury administratora oraz wiedzę o dokonywanych czynnościach przetwarzania a także o systemach informatycznych oraz o potrzebach administratora w zakresie bezpieczeństwa i ochrony danych,
3. IOD jest zatrudniony na podstawie umowy cywilno-prawnej podpisanej z Zakładem Elektronicznej Techniki Obliczeniowej Sp. z o.o. w Koszalinie i został powołany dokumentem „Wyznaczenie Inspektora Ochrony Danych".
4. IOD podlega bezpośrednio kierownikowi jednostki organizacyjnej.
5. Administrator Danych zapewnia dla IOD zasoby niezbędne do wykonywania obowiązków.
6. IOD wykonuje obowiązki wskazane w art. 39 RODO.

§ 3 Zasady ochrony przetwarzania danych osobowych

Administrator Danych przetwarza dane osobowe z poszanowaniem następujących zasad:

1. w oparciu o podstawę prawną i zgodnie z prawem,
2. rzetelnie i uczciwie,
3. w sposób przejrzysty dla osoby, której dane dotyczą,
4. w konkretnych celach,
5. tylko niezbędne dane,
6. nie dłużej niż trzeba,
7. zapewniając odpowiednie bezpieczeństwo danych.

§ 4 System ochrony danych

Na system ochrony danych osobowych składają się następujące elementy:

1. zidentyfikowane procesy w których są przetwarzane dane osobowe oraz opis sposobów przetwarzania tych danych,
2. Rejestr Czynności Przetwarzania Danych Osobowych,
3. podstawy prawne przetwarzania danych osobowych,
4. zasady realizacji obowiązku informacyjnego,
5. procedury obsługi praw osób, których dane są przetwarzane,
6. metody zarządzania minimalizacją przetwarzanych danych,
7. procedury zapewniające odpowiedni poziom bezpieczeństwa danych,
8. zasady identyfikacji i obsługi incydentów,
9. zasady powierzania przetwarzania danych podmiotom zewnętrznym,

10. zasady uruchamiania nowych projektów, w ramach których będą przetwarzane dane osobowe.

4.1. Identyfikacja procesów w których są przetwarzane dane osobowe

Administrator Danych zidentyfikował procesy, w których są przetwarzane dane osobowe. Dla każdego procesu zweryfikowano czy nie zachodzi przypadek współadministrowania. W ramach przeprowadzonej inwentaryzacji zostały wskazane grupy informacji przetwarzane w ramach procesu. Dla każdego procesu dokonano analizy związanej z przetwarzaniem szczególnych kategorii danych osobowych oraz ewentualnym profilowaniem. W ramach inwentaryzacji wskazano również aplikacje, które służą do przetwarzania danych.

Zinwentaryzowane procesy zostały opisane w „Rejestrze Czynności Przetwarzania Danych Osobowych".

4.2. Rejestr Czynności Przetwarzania Danych Osobowych

Administrator Danych prowadzi, zgodnie z wymaganiami art. 30 RODO, Rejestr Czynności Przetwarzania Danych Osobowych. Rejestr stanowi formę dokumentowania czynności przetwarzania danych osobowych. Wzór Rejestru Czynności Przetwarzania Danych Osobowych stanowi zał. nr 1 do Polityki.

Administrator Danych przetwarza niektóre dane osobowe na podstawie umów powierzenia przetwarzania. Rejestr dla tych danych prowadzony jest zgodnie z wzorem stanowiącym zał. nr 1a do Polityki.

4.3. Podstawy prawne przetwarzania danych osobowych

Administrator dokumentuje w Rejestrze, o którym mowa w pkt. 4.2. podstawy prawne przetwarzania danych osobowych. W przypadku każdego procesu wskazuje podstawę prawną przetwarzania danych zwykłych i szczególnych kategorii danych osobowych, które wynikają z RODO (np. zgoda, umowa czy obowiązek prawny) i dookreśla je dodatkowymi informacjami np. dla zgody wskazując na jej zakres a w przypadku podstawy prawnej konkretny przepis ustawy branżowej. Podstawy prawne są okresowo weryfikowane.

4.4. Zasady realizacji obowiązku informacyjnego

Przy pozyskiwaniu danych osobowych od osoby, której dane dotyczą Administrator spełnia obowiązek informacyjny opisany w art. 13 RODO.

W przypadku pozyskiwania danych od potencjalnych pracowników, Administrator przekazuje podstawowe informacje dotyczące przetwarzania danych w ogłoszeniu o rozpoczęciu rekrutacji i wskazuje miejsce gdzie jest publikowany pełny tekst klauzuli informacyjnej.

Przy zbieraniu danych od pracowników obowiązek informacyjny realizowany jest przez udostępnienie informacji o przetwarzaniu danych pracownika w formie dokumentu papierowego i potwierdzenie jej odebrania przez złożenie podpisu pod stosownym oświadczeniem.

Sposób realizacji obowiązku informacyjnego dla każdej czynności przetwarzania danych jest wskazany w Rejestrze Czynności Przetwarzania, o którym mowa powyżej.

4.5. Procedury obsługi praw osób, których dane są przetwarzane

W celu właściwej obsługi praw osób, których dane są przetwarzane przez Administratora, została opracowana Procedura obsługi żądań podmiotu danych, która stanowi załącznik nr 2 do niniejszego dokumentu.

4.6. Metody zarządzania minimalizacją przetwarzanych danych

Na minimalizację przetwarzania danych mają wpływ następujące czynniki:
- adekwatność danych w stosunku do celu przetwarzania,
- dostęp do danych tylko dla tych osób i w takim zakresie jak jest to niezbędne,
- przechowywanie danych nie dłużej niż jest to niezbędne.

W ramach wdrażania RODO Administrator zweryfikował zakres pozyskiwanych informacji oraz zakres ich przetwarzania pod kątem adekwatności w stosunku do celu. Osoba odpowiedzialna za dany zbiór jest zobowiązana do okresowego przeglądu pozyskiwanych i przetwarzanych danych osobowych, by zapewnić, że ich zakres nie wykracza ponad niezbędne minimum. W celu wywiązania się z tego zadania należy między innymi zweryfikować, czy nie nastąpiły zmiany w przepisach prawa.

W celu minimalizacji dostępu do danych osobowych Administrator stosuje ograniczenia organizacyjne, fizyczne i logiczne. Ograniczenia organizacyjne realizowane są poprzez odbieranie od pracowników zobowiązań o zachowaniu poufności i określanie zakresu upoważnień do przetwarzania danych. Ograniczenia fizyczne wynikają z reglamentacji dostępu do pomieszczeń i dokumentów. Ograniczenia logiczne realizowane są przez nadawanie odpowiednich uprawnień dostępowych do systemów, w których są przetwarzane dane osobowe. Uprawnienia dostępowe są aktualizowane przy zmianie stanowiska lub roli pracownika w procesie przetwarzania danych. Administrator zapewnia, że przynajmniej raz do roku dokonuje przeglądu użytkowników systemów i nadanych im uprawnień. Szczegółowe zasady zarządzania uprawnieniami zostały opisane w Procedurze nadawania i zmiany uprawnień.

Administrator zarządza cyklem życia dokumentów przez okresowe przeglądy i ich niszczenie w bezpieczny sposób po upływie okresu ich przechowywania.

4.7. Procedury zapewniające odpowiedni poziom bezpieczeństwa

Administrator zapewnia odpowiedni poziom bezpieczeństwa danych osobowych przez:

- zapewnienie odpowiedniego stanu wiedzy o bezpieczeństwie i zagrożeniach wynikających z przetwarzania danych osobowych (szkolenia pracowników),

- okresowe przeprowadzanie szacowania ryzyka i dobór możliwych do zastosowania zabezpieczeń technicznych i organizacyjnych zgodnie z Instrukcją zarządzania ryzykiem,

- weryfikację skuteczności wdrożonych zabezpieczeń.

Administrator dokonuje oceny skutków dla ochrony danych w tych operacjach, które wskazuje organ nadzorczy.

4.8. Zasady identyfikacji i obsługi incydentów

Administrator przyjął zasady zobowiązujące wszystkich pracowników do powiadamiania bezpośredniego przełożonego i IOD o stwierdzeniu podatności systemu ochrony danych lub wystąpieniu incydentu bezpieczeństwa. Zasady te zostały opisane w Instrukcji zgłaszania i obsługi incydentów.

4.9. Zasady powierzania przetwarzania danych podmiotom zewnętrznym

Administrator opracował ankietę, na podstawie której weryfikuje firmy, z którymi zamierza podpisać umowy powierzenia przetwarzania danych osobowych (zał. nr 3 do Polityki). Weryfikacja firm ma zapewnić, że podmioty przetwarzające dają wystarczające gwarancje bezpiecznego przetwarzania danych osobowych. Jeżeli współpraca z firmą trwała przynajmniej rok, przed wejściem w życie niniejszego dokumentu i nie odnotowano żadnych incydentów bezpieczeństwa, to Administrator może odstąpić od przeprowadzania ankiety.

Administrator opracował wzór umowy powierzenia przetwarzania danych osobowych, która stanowi załącznik nr 4 do Polityki.

Administrator prowadzi rejestr umów, na podstawie których powierzył przetwarzanie danych podmiotom zewnętrznym.

4.10. Zasady uruchamiania nowych projektów, w ramach których będą przetwarzane dane osobowe

W przypadku uruchamiania nowych projektów związanych z przetwarzaniem danych osobowych administrator zapewnia, że uwzględnia w nich zagadnienia związane z bezpieczeństwem i minimalizacją przetwarzanych danych.

§ 5 Postanowienia końcowe

1. Każdy pracownik przed dopuszczeniem do przetwarzania danych osobowych jest przeszkolony w zakresie RODO i wewnętrznych regulacji dotyczących ochrony danych osobowych.
2. Zbiór podstawowych zasad bezpiecznego przetwarzania danych osobowych został zapisany w Regulaminie ochrony danych osobowych (Zał. nr 5 do Polityki).
3. Po zapoznaniu się z zasadami ochrony danych osobowych, pracownik potwierdza znajomość tych zasad i deklaruje ich stosowanie.