Załącznik do Zarządzenia
nr 16/2022 z dnia 19.12.2022 r.
Dyrektora Przedszkola nr 6 w Elblągu

Polityka Bezpieczeństwa Przetwarzania Danych Osobowych i Informacji

Przedszkole nr 6 w Elblągu

Elbląg, 2022 r.

Spis treści

§ 1

Podstawy prawne opracowania dokumentu

1. Niniejszy dokument stanowi Politykę Bezpieczeństwa Informacji w Przedszkolu nr 6 przy ul. Browarnej 13 w Elblągu zwaną dalej Polityką i jest wypełnieniem obowiązku wynikającego z:
    - 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 (ogólne rozporządzenie o ochronie danych lub RODO),
    - Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych,
    - Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla systemów teleinformatycznych.
2. Polityka określa w szczególności zadania i obowiązku administratora danych oraz zasady ochrony i organizacji przetwarzania danych osobowych i informacji, w tym opis środków technicznych i organizacyjnych zastosowanych w celu zapewnienia przestrzegania zasad ujętych w art.5 RODO.

§ 2

Definicje

1. **Dane osobowe** — wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, której dane dotyczą; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
2. **RODO** —Rozporządzenie Parlamentu Europejskiego i Rady (UE) 216/679 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.
3. **Ustawa** —ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.
4. **Placówka –**Przedszkole nr 6 w Elblągu, przy ul. Browarna 13, 82-300 Elbląg, NIP 57830888886 REGON 280564702
5. **Polityka bezpieczeństwa** —niniejszy dokument wraz z załącznikami.
6. **Administrator Danych Osobowych (ADO)** — organ, instytucja, jednostka organizacyjna, podmiot lub osoba, która decyduje o celach i środkach przetwarzania danych osobowych.
7. **Inspektor ochrony danych (IOD)** — osoba powołana przez ADO, pełniąca zadania wynikające z art. 39 RODO.
8. **Rozliczalność** — umiejętność wykazania przestrzegania przepisów wynikających z RODO.
9. **Integralność danych** — atrybut zapewniający, że dane osobowe nie zostaną zmienione w sposób nieautoryzowany;
10. **Poufność danych** — właściwość zapewniająca, że dane są przetwarzane wyłącznie przez osoby upoważnione przez administratora;
11. **Adekwatność danych** — przetwarzanie danych osobowych w zakresie minimalnym do wypełnienia celu, dla którego zostały zebrane.
12. **Przetwarzanie danych osobowych** — jakakolwiek operacja na danych osobowych na przykład: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnienie, dopasowanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
13. **Autoryzowane oprogramowanie –** oprogramowanie dopuszczone do eksploatacji przez administratora danych.
14. **Konto użytkownika** – przestrzeń w systemie informatycznym administratora, do której dostęp otrzymuje użytkownik. Konto opatrzone jest hasłem. Nazwa konta stanowi login użytkownika. Login jest unikatowy dla każdego użytkownika systemu i nie może być przypisany żadnemu innemu użytkownikowi.

15. **Hasło** – ciąg znaków znanych wyłącznie osobie uprawnionej, za którego pomocą użytkownik uzyskuje dostęp do systemu informatycznego administratora.
16. **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
17. **Incydent** – zdarzenie mające lub mogące mieć wpływ na bezpieczeństwo przetwarzanych danych.
18. **Prezes UODO** — rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych.

§3
Zakres regulacji zawartych w Polityce

1. Polityka bezpieczeństwa zawiera:
    a) Zbiór regulacji i zasad wprowadzonych do stosowania przez administratora, dotyczących ochrony danych osobowych w sposób zapewniający zgodność przetwarzania z wymaganiami RODO.
    b) Zadania i odpowiedzialności poszczególnych pracowników Placówki w zakresie ochrony danych osobowych.

§ 4
Zasady przetwarzania danych osobowych

1. Dane osobowe są przetwarzane z poszanowaniem następujących zasad:
    a) **Zasady zgodności z prawem**. Wszystkie dane osobowe gromadzone i przetwarzane są przez Szkołę na podstawie przepisów prawa, zgody pomiotu danych lub w celu realizacji umów.
    b) **Zasady rzetelności i przejrzystości.** Dane osobowe są przetwarzane w sposób rzetelny i przejrzysty dla osoby, której dotyczą. Placówka wypełnia obowiązek informacyjny, który pozwala osobie, której dane dotyczą poznać: Administratora Danych Osobowych, cele, środki i podstawy prawne ich przetwarzania oraz długość okresu przetwarzania danych, a także rodzaje przysługujących podmiotom danych praw w związku z przetwarzaniem ich danych osobowych oraz odbiorców ich danych.
    c) **Zasady minimalizacji danych.** Dane gromadzone i przetwarzane są wyłącznie w zakresie określonym przepisami prawa i niezbędnym do osiągnięcia celu wynikającego z przepisów prawa. Rodzaje dokonywanych przetwarzań określa administrator wraz z zakresem danych przypisanym temu przetwarzaniu. Wprowadza się bezwzględny zakaz przetwarzania danych osobowych bez aktualnej podstawy prawnej i poza rodzajami przetwarzań określonymi przez ADO.
    d) **Zasady prawidłowości.** Prawidłowość i aktualność danych osobowych są na bieżąco weryfikowane. Pozyskiwanie danych osobowych może odbywać się wyłącznie od osób, których dane osobowe dotyczą lub organów, które przekazują Placówce dane osobowe na podstawie przepisów prawa.
    e) **Zasady ograniczenia czasowego.** Dane osobowe podlegają przetwarzaniu wyłącznie do momentu osiągnięcia celu, w jakim zostały zebrane. Następnie są one archiwizowane i przechowywane zgodnie z instrukcją kancelaryjną obowiązującą w Placówce. Po upływie wyznaczonego terminu, dokumenty archiwalne podlegają ocenie i brakowaniu z zachowaniem zasady poufności i integralności danych.
    f) **Zasady poufności i integralności.** ADO stosuje organizacyjne i techniczne środki ochrony danych w celu zachowania poufności, dostępności i integralność danych osobowych. Środki te opisano w punkcie 5 niniejszej polityki.
    g) **Zasady rozliczalności.** Przetwarzanie danych osobowych może odbywać się wyłącznie według procedur opracowanych i wdrożonych w Placówce, co podlega weryfikacji podczas audytów przeprowadzanych przez IOD.

§ 5

Procedura nadawania upoważnień do przetwarzania danych osobowych.

1. Pracownik, który w ramach swoich obowiązków służbowych będzie przetwarzała dane osobowe, musi posiadań stosowane upoważnienie do przetwarzania danych osobowych.
2. ADO przed nadaniem nowemu pracownikowi upoważnienia, organizuje dla niego szkolenie z zakresu ochrony danych osobowych i informacji.
3. Szkolenie przeprowadzane jest w dowolnej formie (szkolenie stacjonarne, e-learningowe, szkolenie poprzez rozesłanie materiałów drogą elektroniczną wraz z testem do rozwiązania itp.).
4. Osobie, która ukończyła szkolenie nadawane jest upoważnienie do przetwarzania danych osobowych, zgodnie z art. 29 RODO.
5. Upoważnienie nadawane jest przez osoby upoważnione do działania w imieniu Placówki tj. Dyrektora Dorotę Szepczyńską lub jego zastępców.
6. Wzór upoważnienie stanowi załącznik nr 1.
7. ADO prowadzi ewidencję osób upoważnionych do przetwarzania danych – której wzór stanowi załącznik nr 2.
8. Zakres nadanego pracownikowi upoważnienia może ulegać zmianie (rozszerzeniu/zwężeniu) w związku z pełnieniem przez niego określonych zadań zgodnie z poleceniami przełożonego w zakresie obowiązków oraz w świetle aktualnej umowy o pracę lub umowy cywilno-prawnej, a także w zgodzie z uprawnieniami do systemów informatycznych.
9. Zmiana zakresu wydanego upoważnienia jest odnotowywana w prowadzonej ewidencji upoważnień.
10. Utrata prawa do przetwarzania danych osobowych określonych w upoważnieniu następuje w szczególności w przypadku:
    a) zmiany stanowiska pracy na stanowisko, na którym nie ma konieczności posiadania dostępu do danych osobowych lub w szczególności, gdy ustaje zasadność i celowość dalszego wykonywania prawa do przetwarzania danych w związku ze zmianą realizowanych przez pracownika zadań wynikających z jego indywidualnego zakresu czynności,
    b) umyślnego naruszenia zasad ochrony danych osobowych określonych w przepisach prawa w tym w szczególności w RODO jak również w przypadku naruszenia zasad określonych w wewnętrznych przepisach ADO,
    c) rozwiązania stosunku pracy,
    d) rozwiązania umowy cywilnoprawnej.
11. Utrata prawa do przetwarzania danych osobowych a w konsekwencji odwołanie upoważnienia następuje poprzez jego wycofanie w ewidencji upoważnień.

§6

Udostępnianie/powierzanie przetwarzania danych

1. Udostępnienie danych osobowych instytucjom i osobom spoza Placówki może odbywać się wyłącznie za zgodą ADO i wyłącznie wtedy, gdy jest to wymagane lub dozwolone przepisami prawa.
2. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Wzór wniosku stanowi załącznik nr 3.
3. Powierzenie danych osobowych może nastąpić wyłącznie podmiotowi przetwarzającemu gwarantującemu bezpieczeństwo przetwarzania danych.
4. Umowa powierzenia przetwarzania danych osobowych musi zawierać wszystkie niezbędne regulacje wynikające z art. 28 RODO wraz z deklaracją stosowanych zabezpieczeń wynikających z art. 32 RODO. Umowa powinna zawierać w szczególności:
    a) Określenie ADO i podmiotu przetwarzającego.
    b) Rodzaj przetwarzania (rodzaj operacji wykonywanych na danych osobowych przez podmiot przetwarzający).
    c) Czas trwania przetwarzania.
    d) Charakter i cel przetwarzania.

e) Rodzaj danych osobowych oraz kategorie osób, których dane dotyczą.
f) Polecenie przetwarzania danych osobowych wydane przez administratora.
g) Warunki podpowierzenia danych (wymagana szczegółowa lub ogólna zgoda administratora).
h) Regulacje dotyczące ewentualnego przekazywania danych osobowych do krajów spoza Europejskiego Obszaru Gospodarczego.
i) Określenie i podział obowiązków pomiędzy administratorem a podmiotem przetwarzającym dotyczących zabezpieczania danych osobowych.
j) Regulacje dotyczące zgłaszania naruszeń danych osobowych.
k) Określenie sposobu postępowania z danymi osobowymi po zakończeniu trwania umowy.
l) Określenie warunków przeprowadzania czynności kontrolnych podmiotu przetwarzającego przez administratora, dotyczących przetwarzania danych osobowych mu powierzonych.
m) Informacje o obowiązku powiadomienia administratora przez podmiot przetwarzający, w przypadku, gdy w jego ocenie administrator wydałby mu polecenie niezgodne z prawem.

5. ADO prowadzi ewidencję udostępnień danych – wzór stanowi załącznik nr 4.
6. ADO prowadzi ewidencję powierzenia danych – wzór stanowi załącznik nr 5.

§ 7

Szkolenia z zakresu ochrony danych osobowych

1. Pracownicy przetwarzający dane osobowe zobowiązani są do uzyskania odpowiedniej wiedzy z zakresu bezpieczeństwa przetwarzania danych osobowych, koniecznej do wykonywania zadań służbowych.
2. Obowiązkowi odbycia szkoleń wymienionych w punkcie 1 podlegają wszyscy pracownicy również praktykanci i stażyści odbywający praktykę / staż w Placówce.
3. Każdy z pracowników jest zobowiązany do uczestnictwa w szkoleniu okresowym odbywającym się nie rzadziej niż raz na 3 lata, lub w przypadku wystąpień znaczących zmian w przepisach prawa oraz regulacjach wewnętrznych z tego zakresu.
4. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania – wzór oświadczenia stanowi załącznik nr 6.
5. Szkolenie może odbyć się również za pośrednictwem platformy internetowej. W takim wypadku potwierdzeniem odbycia szkolenia będzie pozytywnie zdany test (min. 60%) poprawnych odpowiedzi.

§8

Postępowanie w sytuacji wystąpienia incydentu lub naruszenia danych osobowych

1. Każdy pracownik jest zobowiązany do zgłaszania wszelkich sytuacji niebezpiecznych, mogących skutkować naruszeniem bezpieczeństwa, danych. Przyjmuje się, że incydent polegający na naruszeniu ochrony danych osobowych prowadzący do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, ujawnienia lub nieuprawnionego dostępu do danych osobowych stanowi naruszenie.
2. W przypadku stwierdzenia incydentu, pracownik zobowiązany jest do zabezpieczenia miejsca zdarzenia i niezwłocznego poinformowania bezpośredniego przełożonego.
3. Dyrektor jednostki i/lub pracownik jednostki zgłaszający incydent powiadamia Inspektora Ochrony Danych o zaistniałej sytuacji.
4. IOD wraz z ADO określają ryzyko naruszenia praw i wolności osób fizycznych, w związku z zaistniałą sytuacją. Inspektor Ochrony Danych przygotowuje raport i przekazuje go dyrektorowi, wraz z propozycją postępowania w zaistniałej sytuacji. Dyrektor podejmuje decyzję o dalszym przebiegu postępowania.

5. Jeżeli zgodnie z decyzją dyrektora, incydent z dużym prawdopodobieństwem może skutkować naruszaniem praw i wolności osób fizycznych, których dane dotyczą, zgłasza ten fakt nie później niż w ciągu 72 godzin Prezesowi Urzędu Ochrony Danych Osobowych, zachowując formę przewidzianą w art. 33 RODO oraz jeżeli jest to możliwie, zawiadamia osoby, których dane dotyczą.
6. W przypadku wadliwego działania systemu informatycznego, użytkowników obowiązuje całkowity zakaz wykonywania jakichkolwiek napraw. Do diagnozowania usterki lub wadliwego działania systemu informatycznego upoważniony jest tylko Dyrektor lub osoba przez niego wyznaczona.
7. ADO prowadzi ewidencję incydentów/naruszeń ochrony danych osobowych (załącznik nr 7).

§9

Zadania i odpowiedzialności osób, biorących udział w przetwarzaniu danych osobowych.

1. Administrator Danych Osobowych:
    a) dokonuje analizy ryzyka nie rzadziej niż raz w roku lub po każdym zdarzeniu mogącym mieć wpływ na bezpieczeństwo danych osobowych. Metodologia przeprowadzonej analizy jest opisana każdorazowo w raporcie z analizy ryzyka,
    b) uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób, których dane przetwarza, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie było zgodne z przepisami prawa i aby móc to wykazać,
    c) powołuje Inspektora Ochrony Danych,
    d) wydaje polecenia i upoważnienia do przetwarzania danych osobowych,
    e) dokonuje oceny skutków dla ochrony danych,
    f) prowadzi rejestr czynności przetwarzania, zgodnie z art. 30 RODO – wzór rejestru stanowi załącznik nr 8.
2. Inspektor Ochrony Danych (IOD):
    a) uczestniczy we wszystkich sprawach dotyczących ochrony danych osobowych, opiniuje projekty aktualizacji dokumentacji bezpieczeństwa z uwzględnieniem zmian w przepisach prawa,
    b) monitoruje przestrzeganie polityk bezpieczeństwa oraz przepisów prawa w zakresie bezpieczeństwa danych osobowych poprzez wykonywanie audytów i wydawanie rekomendacji,
    c) pełni funkcję punktu kontaktowego dla osób, których dane dotyczą,
    d) pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych;
    e) prowadzi szkolenia nowych pracowników z zakresu zasad bezpieczeństwa danych osobowych przyjętych w Placówce na wniosek Dyrektora,
    f) udziela konsultacji administratorowi oraz pracownikom z zakresu udostępniania i ochrony danych osobowych,
    g) udziela na żądanie rekomendacji, co do oceny skutków dla ochrony danych.
3. Pracownik:
    a) zobowiązany jest do zapoznania się z wszystkimi procedurami, zarządzeniami i politykami bezpieczeństwa danych osobowych wdrożonymi w Placówce,
    b) przetwarza dane osobowe wyłącznie na polecenie i z upoważnienia Dyrektora,
    c) odpowiada za zabezpieczenie dokumentów oraz systemu informatycznego w zakresie realizowanych zadań,
    d) jest zobowiązany do zachowania w tajemnicy informacji pozyskanych w związku z wykonywaną pracą oraz przetwarzanymi danymi,
    e) bez zgody swojego przełożonego nie może wynosić, przekazywać w jakiejkolwiek formie i w jakikolwiek sposób dokumentów i danych poza budynek jednostki,
    f) zobowiązany jest do natychmiastowego zgłaszania przełożonemu wszystkich zauważonych zdarzeń zagrażających bezpieczeństwu ludzi, danych i mienia,

g) bez zgody przełożonego nie może instalować żadnego oprogramowania,
h) nie może używać systemu informatycznego lub jego części i urządzeń do celów niezwiązanych z wykonywana pracą.

§ 10

Prawa osób, których dane są przetwarzane i obowiązek informacyjny Administratora Danych Osobowych

1. Każdej osobie, której dane są zawarte w zbiorach Administratora Danych Osobowych, przysługuje prawo do:
   a) informacji dotyczących celu przetwarzania i okresie przechowywania danych osobowych,
   b) sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych
   c) wniesienia skargi do organu nadzorczego, jeżeli uzna, iż dane są przetwarzane w sposób niewłaściwy,
   d) kontroli przetwarzania danych,
   e) sprostowania dotyczących jej danych osobowych, które są nieprawidłowe oraz uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
2. W przypadku pozyskiwania danych osobowych bezpośrednio od osoby, której one dotyczą, ADO spełnia obowiązki informacyjne przy pozyskiwaniu danych.
3. W przypadku pozyskiwania danych osobowych od innego podmiotu, niż osoba, której one dotyczą, ADO spełnia obowiązek informacyjny wobec osoby, której dane dotyczą.
4. W przypadku przetwarzania danych, za pomocą których nie można zidentyfikować konkretnej osoby fizycznej, ADO spełnia obowiązki informacyjne poprzez zamieszczenie stosownych informacji w miejscu prowadzenia działalności gospodarczej oraz na należących do niego stronach internetowych.
5. Spełnienie obowiązków informacyjnych następuje poprzez przekazanie osobie, której dane dotyczą informacji, o których mowa w art. 13 oraz 14 RODO – wzór klauzuli informacyjnej stanowi załącznik nr 9.
6. W przypadku gdy dane osobowe zbierane są w szerszym zakresie niż wymaga tego cel zbierania danych Administrator Danych Osobowych musi uzyskać zgodę osoby, której dane są przetwarzane na podjęcie przetwarzania – wzór zgody na przetwarzanie danych osobowych stanowi załącznik nr 10.

§ 11

Zasady pracy zdalnej

1. Wykonywanie pracy w trybie Pracy Zdalnej dopuszczalne jest wówczas, gdy pozwalają na to aktualne potrzeby Pracodawcy oraz rodzaj i zakres zadań powierzonych Pracowników.
2. Pracownik może zgłosić pracodawcy chęć podjęcia pracy zdalnej na czas określony, w szczególnych sytuacjach tj. rozprzestrzeniania się chorób zakaźnych, w celu ochrony zdrowia i życia Pracowników lub ze względu na czasową potrzebę innej organizacji pracy.
3. Pracodawca po sprawdzeniu możliwości organizacyjnych może polecić pracownikowi wykonywanie pracy zdalnej na czas określony.
4. Pracownik pozostaje w stałym kontakcie mailowym lub telefonicznym z bezpośrednim przełożonym w godzinach pracy.
5. Warunki i zasady pracy zdalnej, w tym zakres i harmonogram wykonywanej pracy określa Dyrektor.
6. Jeżeli pracownik nie ma możliwości świadczenia pracy zdalnej z zapewnieniem właściwych zabezpieczeń, w szczególności ze względu na siłę wyższą (np. brak prądu lub Internetu), niezwłocznie zgłasza to pracodawcy i postępuje zgodnie z jego instrukcjami.
7. Pracownik wykonuję pracę zdalną zgodnie z zasadami bezpieczeństwa informacji, w tym danych osobowych obowiązujących w jednostce.

8. Niedozwolone jest podejmowanie pracy zdalnej w miejscach publicznych tj. kawiarnie, restauracje, galerie handlowe, gdzie osoby postronne mogłyby usłyszeć fragmenty służbowych rozmów lub zapoznać się z fragmentami wykonywanej pracy.
9. Pracując w domu należy zapewnić, aby domownicy nie mieli wglądu w wykonywaną pracę, w szczególności poprzez właściwe ustawienie ekranu komputera, a także zapewnienie pracy z dokumentami w sposób uniemożliwiający wgląd.
10. W przypadku korzystania z domowej sieci Wifi, należy upewnić się, że została ona skonfigurowana w sposób minimalizujący ryzyko włamania, w szczególności:
    a) korzystanie z Internetu powinno wymagać uwierzytelnienia, np. poprzez hasło,
    b) hasło dostępu powinno składać się z co najmniej 8 znaków, w tym z dużych i małych liter oraz cyfr i znaków specjalnych,
    c) jeśli to możliwe, należy zmienić login do panelu administracyjnego routera na własny.
    d) dostęp do panelu administracyjnego routera jest możliwy wyłącznie z urządzeń znajdujących się w sieci domowej,
    e) został zmieniony domyślny adres routera na inny.
11. Minimalne wymagania, jakie powinno spełniać urządzenie służące do pracy zdalnej w zakresie bezpieczeństwa:
    a) na urządzeniu jest legalne i aktualne oprogramowanie,
    b) zostały włączone automatyczne aktualizacje,
    c) została włączona zapora systemowa,
    d) został zainstalowany i działa w tle program antywirusowy,
    e) zalogowanie do systemu operacyjnego wymaga uwierzytelnienia, np. poprzez indywidualny login i hasło użytkownika, kod PIN,
    f) wyłączono autouzupełnianie i zapamiętywanie hasła w przeglądarce internetowej,
    g) został zainstalowany program umożliwiający zaszyfrowanie i odszyfrowanie danych (np. 7-zip),
    h) zostało ustawione automatyczne blokowanie urządzenia po dłuższym braku aktywności,

§ 12

Postanowienia końcowe

1. Polityka bezpieczeństwa przetwarzania danych stanowi tajemnicę instytucji Administratora Danych Osobowych i podlega ochronie przewidzianej przepisami prawa.
2. Zapoznanie się i wdrożenie postanowień Polityki Bezpieczeństwa oraz wszystkich jej załączników stanowi obowiązek każdej osoby dopuszczonej do przetwarzania danych w jednostce.
3. Polityka bezpieczeństwa obowiązuje od dnia jej zatwierdzenia przez Administratora Danych Osobowych.

Spis załączników:

Załącznik nr 1 wzór upoważnienie do przetwarzania danych;
Załącznik nr 2 wzór ewidencji nadanych upoważnień;
Załącznik nr 3 wzór wniosku o udostępnienie danych;
Załącznik nr 4 wzór ewidencji udostępnień danych;
Załącznik nr 5 wzór ewidencji powierzenia danych;
Załącznik nr 6 wzór oświadczenia pracownika;
Załącznik nr 7 wzór ewidencji incydentów/naruszeń ochrony danych osobowych
Załącznik nr 8 wzór rejestru czynności przetwarzania;
Załącznik nr 9 wzór ogólnej klauzuli informacyjnej;
Załącznik nr 10 wzór zgody na przetwarzanie danych.

Załącznik nr 1
Do Polityki Bezpieczeństwa Informacji

Elbląg, dnia……...r

……..
(pieczęć)

WZÓR

Upoważnienie nr …….
do przetwarzania danych osobowych

Z dniem …… na podstawie art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dn. 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 (RODO), niniejszym upoważniam do przetwarzania danych osobowych
Panią/Pana*…….…….
zatrudnioną/zatrudnionego* na stanowisku……

Zakres upoważnienie:

Lp.	Nazwa zbioru danych lub rodzaj i zakres czynności	Zakres uprawnień	Forma przetwarzania danych
1.	Nazwa zbioru danych wg wewnętrznej ewidencji	np. Bez ograniczeń/podgląd danych/udostępnianie danych/zbieranie danych/wprowadzania danych/edycja danych	Np. Forma papierowa/elektroniczna
2.			

Równocześnie zobowiązuje Pana/Panią do przestrzegania przepisów dotyczących ochrony danych osobowych określonych przepisami RODO, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz dokumentacją wdrożoną przez administratora danych.
Niniejsze upoważnienie zostało nadane na czas* określony, tj. do dnia……../ na czas nieokreślony i traci moc z chwilą rozwiązania umowy o pracę/współpracy*.

Przyjąłem do wiadomości:

……. …….
Podpis upoważnionego *Podpis Administratora Danych*

*niepotrzebne skreślić

Załącznik nr 2
Do Polityki Bezpieczeństwa Informacji

(pieczęć)

Rejestr Upoważnień

l.p.	Nr upoważnienia	Imię i nazwisko	Stanowisko/ pełniona rola	Data wydania upoważnienia	Okres obowiązywania upoważnienia	Zbiór danych, do których osoba została upoważniona	Czynności, do których osoba została upoważniona (Bez ograniczeń, podgląd danych, Wprowadzenie danych, Edycja danych)	Forma przetwarzanych danych (elektroniczna /Papierowa)	Nazwa systemu informatycznego, do których dana osoba otrzymała dostęp

Załącznik nr 3
Do Polityki Bezpieczeństwa Informacji

WZÓR

Wniosek o udostępnienie danych osobowych

1. Wniosek do

_____

_____

(dokładna nazwa administratora danych lub podmiotu przetwarzającego)

2. Wnioskodawca

_____

_____

(nazwa firmy/imię i nazwisko, adres siedziby/zamieszkania, NIP, REGON, dane do korespondencji)

3. Dane osoby reprezentującej wnioskodawcę

_____

_____

(imię i nazwisko, stanowisko, nr telefonu)

4. Dane osoby, której wniosek dotyczy

_____

_____

(wnioskodawca wskazuje te dane o osobie, której wniosek dotyczy, które są mu znane i które pozwolą na jej wyszukanie we wskazanym rejestrze)

5. Podstawa prawna upoważniająca wnioskodawcę do uzyskania danych:

1) _____
2) _____

6. Cel przetwarzania danych:

1) _____
2) _____

7. Nazwa zbioru, z którego mają być udostępnione dane osobowe lub informacje umożliwiające zidentyfikowanie dokumentów, w których występowały dane osobowe:

1) _____
2) _____

8. Zakres wymaganych danych, jakie mają być udostępnione:

1) _____
2) _____

9. Forma doręczenia udostępnianych danych osobowych:

_____

_____

10. Lista załączników do wniosku:

1) _____
2) _____
3) _____

Oświadczam, że
** uzyskane dane będą wykorzystywane wyłącznie do celu, dla którego zostały udostępnione,*
** Wnioskodawca posiada zabezpieczenie techniczne i organizacyjne właściwe dla przetwarzania danych osobowych, w szczególności uniemożliwiające dostęp osób nieuprawnionych do przetwarzania danych osobowych i wykorzystania danych niezgodnie z celem ich uzyskania.*

.....

(miejscowość, data i podpis osoby wnioskującej lub upoważnionej przez wnioskodawcę)

Wypełnia administrator danych

Decyzja administratora danych	Wyrażam zgodę / nie wyrażam zgody* na udostepnienie danych. *(niepotrzebne skreślić)*
Data udostępnienia danych	
Nazwa zbioru, z którego udostępniono dane	
Zakres udostępnionych danych	

……
Data, miejscowość, Podpis administratora danych lub podmiotu przetwarzającego

Załącznik nr 4
Do Polityki Bezpieczeństwa Informacji

WZÓR

Ewidencja udostępniania danych osobowych

Przedszkole nr 6 w Elblągu

l.p.	Data udostępnienia danych	Podmiot, któremu dane udostępniono	Nazwa zbioru, z którego udostępniono dane	Podstawa prawna udostępnienia danych	Zakres udostępnionych danych

WZÓR

Ewidencja powierzenia danych
Przedszkole nr 6 w Elblągu

Lp.	Nazwa oraz siedziba podmiotu	Data powierzenia	Nazwa zbioru danych	Cel powierzenia
1.	Np. Elbląskie Centrum Usług Wspólnych, ul. Saperów 14C, 82-300 Elbląg	01.09.2021 r.	…… …… ……	Realizacja zadań statusowych Elbląskiego Centrum Usług Wspólnych na podstawie Uchwały nr VIII/240/2019 Rady Miejskiej w Elblągu z dnia 28 listopada 2019 r. w sprawie utworzenia samorządowej jednostki organizacyjnej „Elbląskie Centrum Usług Wspólnych”, nadania jej statutu oraz wspólnej obsługi jednostek Gminy Miasta Elbląg.
2.				
3.				

Załącznik nr 6
Do Polityki Bezpieczeństwa Informacji

Elbląg, dnia…….. r.

(Pieczęć)

WZÓR

Oświadczenie

Oświadczam, iż zapoznałem/am się z przepisami dotyczącymi ochrony danych osobowych oraz wdrożonymi przez Przedszkole nr 6 w Elblągu, w szczególności *Polityką Bezpieczeństwa Informacji i Instrukcją Zarządzania Systemem Informatycznym.*

Oświadczam ponadto, iż zobowiązuję się do:

a) zachowania w tajemnicy danych osobowych, do których uzyskałem dostęp w związku ze stosunkiem pracy lub wykonywaniem zobowiązań umownych u administratora danych w trakcie wykonywania obowiązków służbowych oraz po ustaniu stosunku pracy.
b) niewykorzystywania danych osobowych do celów innych, niż te co do których zostały zgromadzone przez administratora danych.
c) zachowania w tajemnicy metod i zasad zabezpieczania danych osobowych u administratora danych.
d) korzystania wyłącznie z oprogramowania i sprzętu dostarczonego przez administratora danych.
e) należytej dbałości o oprogramowanie i sprzęt administratora danych.

Oświadczam, iż w przypadku niestosowania się do powyższych zobowiązań, jestem świadomy/a odpowiedzialności pracowniczej lub odpowiedzialności wynikającej ze zobowiązań umownych, a także odpowiedzialności karnej w przypadku naruszenia przepisów RODO lub Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.
Zobowiązuje się także do natychmiastowego informowania Administratora Danych Osobowych o wszelkich naruszeniach dotyczących ochrony danych osobowych, które będą mi znane.

…….
Data, podpis pracownik

Załącznik nr 7
Do Polityki Bezpieczeństwa Informacji

(pieczęć)

REJESTR INDYDENTÓW

Nr raportu	Osoba		Podjęte działania (zaznaczyć właściwe „x”)			Data ustania zagrożenia	Uwagi
	zgłaszająca	powodująca naruszenie	korekcyjne	korygujące	zapobiegawcze		

Załącznik nr 8
Do Polityki Bezpieczeństwa Informacji

WZÓR

REJESTR CZYNNOŚCI PRZETTWARZANIA

Przedszkole nr 6 w Elblągu

Nazwa administratora danych: ……, 82-300 Elbląg	dane:	tel:	e-mail:
Przedstawiciel administratora danych: Dyrektor jednostki -	dane:	tel:	e-mail:
Inspektor Ochrony Danych:	dane:	tel:	e-mail:

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Zbiór danych	cel przetwarzania/czynność przetwarzania	podstawa przetwarzania	Kategoria osób, których dane dotyczą	Kategoria danych	Kategoria odbiorców danych (w tym procesorów danych)	Okres przechowywania danych *(jeżeli do możliwe)*	źródła pozyskania danych	Przekazywanie do państw trzecich	Nazwa podmiotu przetwarzającego i dane kontaktowe *(jeżeli to możliwe)*	Nazwa współadministratora i dane kontaktowe *(jeżeli to możliwe)*	data ostatniej aktualizacji

TECHNICZNE I ORGANIZACYJNE ŚRODKI BEZPIECZEŃSTWA

Nazwa zbioru	Forma przetwarzania	Wdrożone środki bezpieczeństwa			
	Elektroniczna				
	Papierowa				

WZÓR

Klauzula obowiązku informacyjnego
Ogólna

1. Administratorem Pani/Pana danych osobowych jest: Przedszkole nr 6 przy ul. Browarna 13, 82-300 Elbląg, reprezentowana przez Dyrektora.
2. Administrator powołał Inspektora Ochrony Danych, z którym można się kontaktować pod adresem: iod@ecuw.elblag.eu lub nr tel. 55 625 68 08/09
3. Pani/Pana dane osobowe przetwarzane są na podstawie art. 6 ust. 1 lit. c Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE w tym, w celu realizacji zadań ustawowych oraz określonych w Ustawie PRAWO OŚWIATOWE na podstawie, której funkcjonuje Przedszkole nr 6 w Elblągu.
4. Dane osobowe przechowywane są przez okres niezbędny do realizacji celów wskazanych w pkt. 3, a następnie w przypadkach, w których wymagają tego przepisy ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, przez czas określony w tych przepisach;
5. Podanie danych jest:
    - obowiązkowe, w sytuacji, gdy przesłankę przetwarzania danych osobowych stanowi przepis prawa,
    - dobrowolne, w sytuacji, gdy przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą;
6. Dane osobowe mogą być przekazywane wyłącznie podmiotom uprawnionym na podstawie przepisów prawa oraz tym, którym Administrator powierzył przetwarzanie danych osobowych;
7. Posiadają Państwo prawo dostępu do treści danych, ich sprostowania, cofnięcia zgody na przetwarzanie danych osobowych w przypadku przetwarzania danych na podstawie zgody lub ich usunięcia, ograniczenia przetwarzania, przenoszenia danych oraz wniesienia skargi do Prezesa Urzędu Ochrony Danych (PUODO).

Załącznik nr 10
Do Polityki Bezpieczeństwa Informacji

WZÓR

Zgoda na przetwarzanie danych osobowych

Ja niżej podpisana/podpisany na podstawie art. 6 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 (RODO) wyrażam zgodę na przetwarzanie moich danych osobowych przez *Przedszkole nr 6* w Elblągu, w postaci…….. . …….. w celu ……

Jednocześnie oświadczam, iż zapoznałem się z informacjami dotyczącymi przetwarzania moich danych osobowych zgodnie z art. 13 i 14 RODO, załączonymi do niniejszego oświadczenia i/lub dostępnymi na stronie internetowej: http://przedszkole6.elblag.eu/

.....

Miejscowość, data, czytelny podpis