Polityka bezpieczeństwa
w Publicznym Przedszkolu Nr 1
w Pile

ZARZĄDZENIE

DYREKTORA PUBLICZNEGO PRZEDSZKOLA NR 1 W PILE

z dnia 11 grudnia 2018 r.

w sprawie ochrony przetwarzanych danych osobowych w Publicznym Przedszkolu Nr 1 w Pile.

Na podstawie art. 24 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 zarządza się, co następuje:

§ 1. Wprowadza się System Ochrony Danych Osobowych w Publicznym Przedszkolu Nr 1 w Pile, zwany dalej „systemem".

§ 2. W skład systemu wchodzą następujące dokumenty:

1.Polityka bezpieczeństwa w Publicznym Przedszkolu Nr 1 w Pile, stanowiąca załącznik nr 1 do niniejszego zarządzenia.

2.Instrukcja zarządzania systemami informatycznymi w Publicznym Przedszkolu Nr 1 w Pile, stanowiąca załącznik nr 2 do niniejszego zarządzenia.

§ 3. Wprowadza się dokumentowanie przetwarzania danych osobowych w oparciu o Wykaz wzorów, stanowiący załącznik nr 3 do niniejszego zarządzenia.

§ 4. Zarządzenie wchodzi w życie z dniem podjęcia.

11.12.2018 r.	Alicja Smarz
.....	.....
(miejscowość, data)	(podpis i pieczęć dyrektora)

Załącznik Nr 1
do zarządzenia
Dyrektora Publicznego Przedszkola Nr 1 w Pile
z dnia 11.12.2018 r.

Polityka bezpieczeństwa

w Publicznym Przedszkolu Nr 1 w Pile

I.POSTANOWIENIA WSTĘPNE

1.„Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, w Publicznym Przedszkolu nr 1 w Pile", jest dokumentem zwanym dalej polityką bezpieczeństwa, który określa zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym ujawnieniem.

2.Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, aktach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

3.Polityka bezpieczeństwa w zakresie zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, zawiera:

3.1.identyfikację zasobów systemu tradycyjnego i informatycznego,

3.2.wykaz pomieszczeń, tworzący obszar, w którym przetwarzane są dane osobowe,

3.3.wykaz zbiorów danych osobowych oraz programy zastosowane do przetwarzania tych danych,

3.4.opis struktury zbiorów danych i sposoby ich przepływu,

3.5.środki techniczne i organizacyjne, służące zapewnieniu poufności przetwarzanych danych.

4.Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych w Publicznym Przedszkolu Nr 1 w Pile, jak i innych, np. studentów, odbywających w nim praktyki pedagogiczne.

5.„Dane osobowe" są to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Możliwa do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny (np. PESEL, NIP) albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

6.Odpowiedzialność za powierzone dane osobowe, ponoszą wszyscy pracownicy przedszkola, mający dostęp do danych osobowych w ramach swych obowiązków służbowych.

7.**„Polityka bezpieczeństwa" jest to zestaw praw, reguł i praktycznych doświadczeń regulujących**

sposób zarządzania, ochrony i dystrybucji zasobów w danych osobowych „Polityka bezpieczeństwa" opisuje działania, które w najbardziej efektywny sposób pozwolą osiągnąć postawiony cel, jakim jest ochrona podstawowych prawa i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych.

8. W celu zapewnienia bezpieczeństwa przetwarzanych danych wymaga się, aby wszyscy jego użytkownicy byli świadomi konieczności ochrony wykorzystywanych zasobów. Konsekwencją nie stosowania przez pracownika środków bezpieczeństwa określonych w instrukcjach wewnętrznych może być zniszczenie części lub całości systemów informatycznych, utrata poufności, autentyczności, straty finansowe, jak również utrata wizerunku.
9. **Pracownicy są odpowiedzialni za bezpieczeństwo danych, do których mają dostęp. W szczególności w systemach informatycznych odpowiadają oni za poprawne wprowadzanie informacji do tych systemów oraz za użycie, zniszczenie lub uszkodzenie** sprzętu oraz znajdujących się na nim danych i oprogramowania.

I.DEFINICJE

Ilekroć w „Polityce bezpieczeństwa" jest mowa o:

1. **Administratorze danych (ADO)** – rozumie się przez to Publiczne Przedszkole Nr 1, reprezentowane przez Dyrektora, decydującego o celach i środkach przetwarzania danych,
2. **Inspektorze ochrony danych (IOD)** – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków inspektora ochrony danych,
3. **Prezesie Urzędu Ochrony Danych Osobowych** – Prezes Urzędu jest organem nadzorczym w rozumieniu 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 (Dziennik Urzędowy UE - 4.5.2016 L 119/3).
4. **Danych osobowych** – są to dane o zidentyfikowanej, bądź możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą).
5. **Danych osobowych szczególnej kategorii** - dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
6. **Osoba fizyczna** - to prawne określenie człowieka, jako podmiotu stosunku cywilnoprawnego. Osoba fizyczna rozpoczyna swój byt prawny w chwili urodzenia, a kończy go w chwili śmierci. Osoby fizyczne posiadają zdolność prawną, a także po spełnieniu określonych warunków zdolność do czynności prawnych.

7. **Osoba możliwa do zidentyfikowania** – to osoba fizyczna, którą można pośrednio lub bezpośrednio zidentyfikować, w szczególności za pomocą identyfikatora takiego jak imię, nazwisko, nr identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
8. **RCPD (Rejestr czynności)** - oznacza Rejestr Czynności Przetwarzania Danych Osobowych, stosowany przez Administratora.
9. **RKCPD (Rejestr kategorii)** - oznacza Rejestr Kategorii Czynności Przetwarzania Danych Osobowych, stosowany przez podmiot przetwarzający.
10. **Przetwarzaniu danych osobowych** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
11. **Ochronie danych osobowych** - dołożenie wszelkich starań celem zabezpieczenia danych osobowych osoby, której dane dotyczą poprzez zapewnienie szczególnych środków technicznych i organizacyjnych do ochrony danych. Zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
12. **Zautomatyzowanym przetwarzaniu danych osobowych** – przetwarzanie danych osobowych w systemach informatycznych bez udziału człowieka (np. automatyczne podejmowanie decyzji).
13. **Zgoda na przetwarzanie danych osobowych** – jest to dobrowolne, sprecyzowane, świadome i jednoznaczne określenie woli osoby, której dane dotyczą, wyrażone w formie pisemnego oświadczenia złożonego na formularzu w formie tradycyjnej lub przesłanego za pośrednictwem poczty elektronicznej.
14. **Ryzyko** - to możliwość zaistnienia zdarzenia, które może mieć wpływ na realizację założonych celów w zakresie ochrony danych osobowych. Ryzyko mierzone jest siłą skutku oddziaływania oraz prawdopodobieństwem jego wystąpienia.
15. **Zarządzanie ryzykiem** - jest to kilkuetapowy proces polegający na wyszukaniu i nazwaniu każdego ryzyka zagrażającego danym przetwarzanym przez Administratora wraz ze źródłami, przyczynami i wstępnym określeniem szkód jakie im towarzyszą. Następnie na szacowaniu prawdopodobieństwa wystąpienia zdefiniowanych rodzajów ryzyka, określenie wartości prawdopodobnych strat, a następnie minimalizacja tych ryzyk.

16. **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
17. **Ustawie** – Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych,
18. **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
19. **identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
20. **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osobę upoważnioną do przetwarzania danych; osobę, której powierzono przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
21. **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to pracownika przedszkola, który upoważniony został do przetwarzania danych osobowych przez dyrektora przedszkola na piśmie,
22. **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
23. **serwisancie** – rozumie się przez to firmę lub pracownika firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego,
24. **sieci publicznej** – rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych,
25. **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
26. **przedszkole** – rozumie się przez to Publiczne Przedszkole Nr 1 w Pile,
27. **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
28. **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
29. **użytkowniku** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło,
30. **Incydencie (naruszeniu zasad ochrony danych osobowych)** - to incydent polegający na przypadkowym lub niezgodnym z prawem modyfikowaniu, niszczeniu, utracie danych, nieuprawnionym ujawnieniu ich treści lub nieuprawnionym dostępie do danych osobowych.

31. **Zagrożeniu** - są to czynnymi zewnętrzne lub wewnętrzne mogące prowadzić do wystąpienia incydentu i mogące mieć negatywny wpływ na proces przetwarzania danych osobowych.
32. **Podatność** – jest to potencjalnie słaby punkt (luka w bezpieczeństwie), który może być wykorzystany przez zagrożenie, doprowadzając do negatywnych skutków.
33. **Integralność** – to właściwość oznaczająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany. A w przypadku systemów informatycznych, właściwość umożliwiająca systemowi realizację zamierzonej funkcji w nienaruszony przez nieautoryzowane manipulacje (celowe lub przypadkowe) sposób.
34. **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

III.ZAGADNIENIA DOTYCZĄCE OCHRONY DANYCH OSOBOWYCH

Prezes Urzędu Ochrony Danych Osobowych (PUODO)

Prezes Urzędu Ochrony Danych Osobowych jako organ nadzorczy w rozumieniu Rozporządzenia:

1. monitoruje i egzekwuje stosowanie niniejszego rozporządzenia;
2. upowszechnia w społeczeństwie wiedzę o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk. Szczególną uwagę poświęca działaniom skierowanym do dzieci;
3. doradza, zgodnie z prawem państwa członkowskiego, parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie aktów prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem;
4. upowszechnia wśród administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia;
5. udziela osobie, której dane dotyczą, na jej żądanie informacji o wykonywaniu praw przysługujących im na mocy niniejszego rozporządzenia, a w stosownym przypadku współpracuje w tym celu z organami nadzorczymi innych państw członkowskich;
6. rozpatruje skargi wniesione przez osobę, której dane dotyczą, lub przez podmiot, organizację lub zrzeszenie zgodnie z art. 80 Rozporządzenia, w odpowiednim zakresie prowadzi postępowania w przedmiocie tych skarg i w rozsądnym terminie informuje skarżącego o postępach i wynikach tych postępowań, w szczególności jeżeli niezbędne jest dalsze prowadzenie postępowań lub koordynacja działań z innym organem nadzorczym;

7. współpracuje z innymi organami nadzorczymi, w tym dzieli się informacjami oraz świadczy wzajemną pomoc, w celu zapewnienia spójnego stosowania i egzekwowania niniejszego rozporządzenia;
8. prowadzi postępowania w sprawie stosowania niniejszego rozporządzenia, w tym na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego;
9. monitoruje zmiany w stosownych dziedzinach, o ile zmiany te mają wpływ na ochronę danych osobowych, w szczególności monitoruje rozwój technologii informacyjno-komunikacyjnych i praktyk handlowych;
10. przyjmuje standardowe klauzule umowne, o których mowa w art. 28 ust. 8 i art. 46 ust. 2 lit. d. Rozporządzenia;
11. ustanawia i prowadzi wykaz związany z wymogiem dokonania oceny skutków dla ochrony danych na mocy art. 35 ust. 4 Rozporządzenia;
12. udziela zaleceń, o których mowa w art. 36 ust. 2 Rozporządzenia, dotyczących operacji przetwarzania;
13. zachęca do sporządzania kodeksów postępowania zgodnie z art. 40 ust. 1 Rozporządzenia, wydaje opinie na ich temat oraz zatwierdza te kodeksy, w których znajdują się odpowiednie zabezpieczenia, na mocy art. 40 ust. 5 Rozporządzenia;
14. zachęca do ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych oraz znaków jakości i oznaczeń z tej dziedziny zgodnie z art. 42 ust. 1 Rozporządzenia, a także zatwierdza kryteria certyfikacji zgodnie z art. 42 ust. 5 Rozporządzenia;
15. gdy ma to zastosowanie – zgodnie z art. 42 ust. 7 Rozporządzenia dokonuje okresowego przeglądu udzielonych certyfikacji;
16. opracowuje i publikuje kryteria akredytacji podmiotu monitorującego kodeksy postępowania na mocy art. 41 Rozporządzenia oraz podmiotu certyfikującego na mocy art. 43 Rozporządzenia;
17. akredytuje podmiot monitorujący kodeksy postępowania na mocy art. 41 Rozporządzenia oraz podmiot certyfikujący na mocy art. 43 Rozporządzenia;
18. wydaje zezwolenia na klauzule umowne i przepisy, o których mowa w art. 46 ust. 3 Rozporządzenia;
19. zatwierdza wiążące reguły korporacyjne na mocy art. 47 Rozporządzenia;
20. bierze udział w pracach Europejskiej Rady Ochrony Danych;
21. prowadzi wewnętrzny rejestr naruszeń niniejszego rozporządzenia i działań podjętych zgodnie z art. 58 ust. 2 Rozporządzenia;
22. wypełnia inne zadania związane z ochroną danych osobowych.

Kontrole PUODO

Kontrolę przeprowadza upoważniony przez Prezesa Urzędu:

1. pracownik Urzędu,
2. członek lub pracownik organu nadzorczego państwa członkowskiego Unii Europejskiej w przypadku, o którym mowa w art. 62 Rozporządzenia – zwany dalej „kontrolującym".

Kontrolujący ma prawo:

1. wstępu w godzinach od 6.00 do 22.00 na grunt oraz do budynków, lokali lub innych pomieszczeń;
2. wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;
3. przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych;
4. żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego;
5. zlecać sporządzanie ekspertyz i opinii.

Działania PUODO w przypadku naruszenie przepisów

Jeżeli na podstawie informacji zgromadzonych w postępowaniu kontrolnym Prezes Urzędu uzna, że mogło dojść do naruszenia przepisów o ochronie danych osobowych, obowiązany jest do niezwłocznego wszczęcia postępowania w sprawie naruszenia przepisów o ochronie danych osobowych.

Administrator danych osobowych (ADO) reprezentowany przez dyrektora przedszkola, realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1.podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych,

2.upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków, oraz odwołuje te upoważnienia lub wyrejestrowuje użytkownika z systemu informatycznego,

3.wyznacza inspektora ochrony danych oraz administratora sieci oraz określa zakres jego zadań i czynności,

4.prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych oraz pozostałą

dokumentację z zakresu ochrony danych, o ile jako właściwą do jej prowadzenia nie wskaże inną osobę,

5.zapewnia we współpracy z inspektorem ochrony danych użytkownikom odpowiednie stanowiska i warunki pracy, umożliwiające bezpieczne przetwarzanie danych,

6.podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur.

Inspektor Ochrony Danych (IOD)

Zgodnie z art. 37 ust. 1 pkt a RODO Publiczne Przedszkole Nr 1 w Pile powołało Inspektora Ochrony Danych (IOD).

Do jego obowiązków należy:

1. Informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie.
2. Monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.
3. Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35.
4. Współpraca z organem nadzorczym.
5. Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
6. Pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.

Osoba upoważniona do przetwarzania danych jest zobowiązana przestrzegać następujących zasad:

1.może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych obowiązków.

Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych,

2. musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji.

3. zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki i instrukcji zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych,

4. stosuje określone przez administratora danych oraz inspektora ochrony danych procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych,

5. korzysta z systemu informatycznego administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcji obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników,

6. zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

Przetwarzanie danych

Przetwarzanie **danych zwykłych**

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

1. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Przetwarzanie **szczególnych kategorii danych**

Przetwarzanie danych jest **zabronione** w przypadku danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

Przetwarzanie tych danych **jest jednak dopuszczalne**, jeżeli:

1. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania danych szczególnych;
2. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
3. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
4. przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe

kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

5. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
6. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
7. 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;
8. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 9 ust. 3 Rozporządzenia;
9. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
10. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 Rozporządzenia, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

III.IDENTYFIKACJA ZASOBÓW SYSTEMU INFORMATYCZNEGO

Struktura informatyczna Publicznego Przedszkola Nr 1 w Pile składa się z sieci wewnętrznej, mieszczącej się w pomieszczeniach przedszkola i jest połączona siecią zbudowaną w oparciu o łącza Asty-net . Informacje przetwarzane w tej strukturze są jawne, ale podlegają ochronie zgodnie z przepisami ustawy i RODO.

IV.WYKAZ POMIESZCZEŃ, TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

1.Przetwarzaniem danych osobowych jest wykonywanie jakichkolwiek operacji na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza tych, które wykonuje się w systemie informatycznym.

2.Dane osobowe przetwarzane są na terenie Centrum Usług Wspólnych, gdzie pracują księgowa i kadrowa obsługujące Publiczne Przedszkole Nr 1 oraz na terenie Publicznego Przedszkola Nr 1.

3.Ze względu na szczególne nagromadzenie danych osobowych szczególnie chronione są następujące pomieszczenia:

3.1.biuro dyrektora przedszkola

3.2.biuro starszego referenta

III.WYKAZ ZBIORÓW DANYCH OSOBOWYCH ORAZ PROGRAMÓW STOSOWANYCH DO PRZETWARZANIA TYCH DANYCH W PUBLICZNYM PRZEDSZKOLU NR 1 W PILE

1. WYKAZ ZBIORÓW

Lp.	Nazwa zbioru danych	Zakres Zbioru- opis	Programy zastosowane do przetwarzania danych/nazwa zasobu danych
1.	**Kandydaci do przedszkola**	Karta zapisu dziecka do przedszkola- informacje dotyczące przyjmowanego	Program Nabór
2.	**Wychowankowie przedszkola**	Dziennik zajęć przedszkola – przebieg pracy dydaktyczno -wychowawczej z dziećmi za dany rok szkolny	Program odpłatności
		Dziennik innych zajęć – pomoc psychologiczno-pedagogiczna udzielana dzieciom	
		Arkusz obserwacji dziecka i wyniki diagnozy	

		przedszkolnej	
		Indywidualne programy wspomagania i korygowania rozwoju	
		Protokoły Rady Pedagogicznej	
		Obowiązek przedszkolny- przekazywania informacji o realizacji obowiązku do szkoły	
		Lista uczestników wycieczek	
		Ubezpieczenie uczniów	
		Opinie i Orzeczenia poradni Psychologiczno-Pedagogicznej	
		Wnioski rodziców o naukę religii	
		Upoważnienia i zgody rodziców i organów zewnętrznych	
		Zaświadczenia i opinie dla rodziców	
		Udział dzieci w konkursach	
		Naliczanie odpłatności za przedszkole	
		System Informacji Oświatowej – dane osobowe dziecka, w tym nr Pesel	SIO
3.	**Pracownicy Przedszkola**	Arkusz Organizacji Przedszkola	AOS
		System Informacji Oświatowej	
		Komisja socjalna- świadczenia dla pracowników	
		Dokumentacja wypadków pracowników- informacje o wypadkach pracowników	SIO
		Awans zawodowy	
		Wykazy premii i innych wynagrodzeń finansowych przyznanych pracownikom	
4.	**Nagrania z monitoringu wizyjnego**	Wizerunek Dane biometryczne	System LINUX Wersja BCS 24.0

2. WYKAZ PROGRAMÓW STOSOWANYCH W PRZEDSZKOLU:

1.SIO- System Informacji Oświatowej,

2.Bankowe konto IPKOBIZNES - CUW i przedszkole

3.Nabór

4.Program odpłatności

5.Arkusz organizacji przedszkola AOS – Vulcan

III.STRUKTURA ZBIORÓW DANYCH, SPOSÓB PRZEPŁYWU DANYCH I ZAKRES ICH PRZETWARZANIA

1. **Zbiór danych „Kandydaci do przedszkola”** obejmuje dane osobowe kandydatów, obiegających się o przyjęcie do przedszkola.
   1.1. Zakres danych tego zbioru to: imię (imiona) i nazwisko kandydata, data i miejsce urodzenia, PESEL, adres zamieszkania, imię i nazwisko rodziców (prawnych opiekunów), ich adres zamieszkania, numer telefonu, dostępny jest dyrektorowi przedszkola, starszemu referentowi i komisji rekrutacyjnej. Dane osobowe kandydatów i ich rodziców znane są członkom komisji rekrutacyjnej i pozostałym osobom, uczestniczącym w procedurze naboru, w dniu ogłoszenia wyników naboru. Wykazy kandydatów, przyjętych do przedszkola, są upubliczniane tzn. wywieszane są listy w przedszkolu w dniu ogłoszenia wyników zawierające: imiona i nazwiska kandydatów. Dane z tego zakresu przetwarzane są za pomocą programu „Nabór”, systemowa obsługa rekrutacji oświatowej, opracowany przez Poznańskie Centrum Superkomputerowo-Sieciowe. Jest on uruchamiany za pomocą identyfikatora i hasła.
   1.2. Dane w formie liczby dzieci przyjętych i nieprzyjętych oraz imiona i nazwiska mogą być udostępniane organowi prowadzącemu przedszkole (Wydziałowi Oświaty, Kultury i Sportu Urzędu Miasta Piły) w celu opracowywania raportów o wynikach naboru kandydatów do pilskich przedszkoli.
2. **Zbiór danych „Wychowankowie przedszkola”** obejmuje dane osobowe dzieci i ich rodziców: imię (imiona) i nazwisko dziecka, data i miejsce urodzenia, adres zamieszkania, PESEL oraz imiona i nazwisko rodziców (prawnych opiekunów), adres zamieszkania, numer telefonu domowego lub do pracy.
   2.1. Zakres pierwszy danych tego zbioru: numer ewidencyjny dziecka, imię (imiona) i nazwisko, data i miejsce urodzenia, adres zamieszkania oraz imiona i nazwiska rodziców (prawnych opiekunów) ucznia – jest dostępny wychowawcom klasowym, dyrektorowi. Dane tego zakresu są udostępniane organowi prowadzącemu przedszkole i organowi nadzorującemu przedszkole w celu przeprowadzenia kontroli. Dane tego zakresu mogą być udostępnione pracownikom NIK, UODO, MEN na podstawie pisemnych upoważnień do przeprowadzenia kontroli, a także policji i straży miejskiej, kuratorom sądowym oraz innym służbom upoważnionym na podstawie przepisów prawa.
   2.2. Zakres drugi danych tego zbioru: imię (imiona) i nazwisko dziecka, data i miejsce urodzenia, imiona i nazwisko rodziców (prawnych opiekunów) oraz adres ich zamieszkania odnosi się do arkuszy obserwacji przedszkola. Dane w nich zawarte przetwarzają wychowawcy klas, a dostęp do nich mają również dyrektor przedszkola, który po zakończonym cyklu kształcenia gromadzi je w teczkach i przechowuje w archiwum przedszkolnym. Dane z zakresu drugiego

mogą być udostępniane tylko przedstawicielom organu nadzorującego przedszkole w celach kontrolnych.

2.3. Zakres trzeci danych osobowych tego zbioru: imiona i nazwisko ucznia, data i miejsce urodzenia, imiona i nazwisko rodziców (prawnych opiekunów) oraz adres zamieszkania i numery telefonów do domu lub do pracy obejmuje dzienniki lekcyjne i jest dostępny wszystkim nauczycielom zatrudnionym w szkole oraz praktykantom, odbywającym w niej praktyki pedagogiczne. Przechowywany jest w sali zajęć w specjalnie szafce zamykanej na klucz. Nie mają do niej dostępu ani dzieci, ani ich rodzice, jak również pozostali pracownicy przedszkola. Po zakończonym roku szkolnym zdaje się je do archiwum przedszkolnego. Dane osobowe z tego zakresu mogą być udostępnione jedynie przedstawicielom organu prowadzącego przedszkole oraz organu nadzorującego w czasie wizytacji lub w sytuacjach interwencyjnych, a także NIK i MEN w celu przeprowadzenia odpowiednich kontroli.

2.4. Zakres czwarty danych tego zbioru obejmuje dane dzieci (w tym dane szczególnych kategorii), tj. imiona i nazwisko dziecka, data i miejsce urodzenia, adres zamieszkania a także ostatnie dane o stanie zdrowia (w tym również zdrowia psychicznego), przedstawione w zaświadczeniach i opiniach, poradni psychologiczno-pedagogicznej, która wnioskuje do dyrektora przedszkola o odroczenie od realizacji obowiązku szkolnego, nauczanie indywidualne, indywidualny tok nauki, obniżenie progu wymagań albo dostosowanie warunków pracy do formy niepełnosprawności dziecka.

2.5. Dostęp do tych danych, które są przetwarzane wyłącznie ręcznie, mają wyłącznie dyrektor przedszkola, nauczyciele pracujący bezpośrednio z dzieckiem oraz specjaliści obejmujący dziecko opieką psychologiczno-pedagogiczną. Mogą być udostępnione organom nadzorującym.

3. **Zbiór danych „Pracownicy przedszkola”** obejmuje dane osobowe byłych i obecnych pracowników przedszkola, tj.: nauczycieli, pracowników administracji i obsługi. Dane te przetwarzane są zarówno ręcznie, jak i w systemie informatycznym.

3.1. Zakres pierwszy danych tego zbioru, tzn. imię i nazwisko wszystkich pracowników oraz ich numery telefonów, dostępne są wszystkim pracownikom przedszkola w gabinecie starszego referenta.

3.2. Zakres drugi tego zbioru, tzn. imię i nazwisko pracownika przedszkola, data i miejsce urodzenia imiona i nazwisko rodziców, adres zamieszkania, wysokość wynagrodzenia, dane dotyczące wynagrodzenia, kwalifikacji zawodowych, wynagrodzenia, przeszeregowań, urlopów i zwolnień lekarskich, numer dowodu osobistego, numer NIP i PESEL, a także dane wrażliwe – informacje o odbytych szkoleniach, o posiadanych dzieciach, zawartym związku małżeńskim, a także dane o stanie zdrowia, wynikające z zaświadczeń lekarskich, wydawanych na podstawie przeprowadzonych badań profilaktycznych (wstępnych, okresowych i kontrolnych) oraz w związku z ubieganiem się nauczyciela o przyznanie

urlopu dla podratowania zdrowia. Dane z zakresu drugiego zamieszczone są w dokumentach teczek akt osobowych pracownika, które przechowywane są w Centrum Usług Wspólnych a dostęp do nich mają:

3.2.1.dyrektor przedszkola,

3.2.2.Centrum Usług Wspólnych

Dane z zakresu drugiego mogą być udostępniane organowi prowadzącemu przedszkole i organowi nadzorującemu przedszkole, a także innym organom prowadzącym kontrolę, w tym zwłaszcza PIP, RIO i sądom powszechnym w związku z prowadzonym postępowaniem.

W systemie informatycznym, funkcjonującym w przedszkolu, dane zbioru „Pracownicy przedszkola" są przetwarzane tylko w drugim zakresie. Na polecenie dyrektora przedszkola pracownik CUW zajmujący się sprawami kadrowymi, przygotowuje w programie umowy o pracę, porozumienia, przeszeregowania, wypowiedzenia, w tym wypowiedzenia zmieniające, informacje o warunkach zatrudnienia, korespondencję w sprawie zatrudnienia i wysokości zarobków lub rozwiązania stosunku pracy i świadectwa pracy. Dane te są niezwłocznie wprowadzane do bazy danych komputera. Dostęp do nich jest możliwy po wprowadzeniu odpowiedniego identyfikatora i hasła pracownika, zajmującego się sprawami kadrowymi.

3.3.Zakres trzeci tego zbioru, tzn. imię i nazwisko pracownika, imiona i nazwiska dzieci oraz współmałżonka, adres zamieszkania, dochody pracownika, dochody współmałżonka, informacje o sytuacji życiowej, rodzinnej i materialnej są udostępniane komisji socjalnej w celu rozpatrywania wniosków pracowników o przyznanie świadczeń socjalnych. Dane te są przetwarzane ręcznie.

3.4.Z teczek akt osobowych pracowników przedszkola dane są przekazywane przez osoby zajmujące się sprawami kadrowymi, dyrektora w sposób tradycyjny do programów SIO – system informacji oświatowej i Arkusza Optivum Vulkan – arkusza organizacyjnego uaktualniane dwa razy do roku -31 marca i 31 września. Wprowadzanie danych do SIO jest możliwe po wprowadzeniu identyfikatora i hasła. Dostęp do tych danych mają organ prowadzący i nadzorujący przedszkole, w przypadku SIO do danych osobowych ma dostęp również MEN.

III.Wykaz zbiorów danych osobowych

1.Przetwarzanych w systemach informatycznych:

1.1.Kandydaci do przedszkola: nabór elektroniczny

1.2.Wychowankowie przedszkola: Naliczanie odpłatności za przedszkole, SIO, Arkusz organizacyjny, nabór elektroniczny,

1.3.Pracownicy przedszkola: SIO, Arkusz Organizacyjny

2.Wykaz zbiorów prowadzonych manualnie:

2.1.Karta zapisu dziecka do przedszkola- informacje dotyczące przyjmowanego

2.2.Dziennik zajęć przedszkola – przebieg pracy dydaktyczno –wychowawczej z dziećmi za dany rok szkolny

2.3.Dziennik innych zajęć – organizacja zajęć dodatkowych (religia)

2.4.Dziennik innych zajęć – pomoc psychologiczno- pedagogiczna udzielana dzieciom

2.5.Arkusz obserwacji dziecka i wyniki diagnozy przedszkolnej

2.6.Indywidualne programy wspomagania i korygowania rozwoju

2.7.Protokoły Rady Pedagogicznej

2.8.Obowiązek przedszkolny- przekazywania informacji o realizacji obowiązku do szkoły

2.9.Lista uczestników wycieczek

2.10.Ubezpieczenie uczniów

2.11.Opinie i Orzeczenia poradni Psychologiczno- Pedagogicznej

2.12.Wnioski rodziców o naukę religii

2.13.Upoważnienia i zgody rodziców

2.14.Zaświadczenia i opinie dla rodziców

2.15.Udział dzieci w konkursach

2.16.Komisja socjalna- świadczenia dla pracowników

2.17.Dokumentacja wypadków pracowników- informacje o wypadkach pracowników

2.18.Awans zawodowy

2.19.Wykazy premii i innych wynagrodzeń finansowych przyznanych pracownikom

2.20.Książka korespondencyjna

III.REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Ważnym elementem Polityki Ochrony Danych jest Rejestr Czynności Przetwarzania Danych Osobowych (RCPD). Identyfikuje on wszystkie procesy dotyczące danych osobowych zachodzące na wszystkich zbiorach, pozwala na kontrolę nad tymi procesami oraz systemami używanymi do ich realizacji.

RCPD stanowi formę dokumentowania czynności przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację jednej z głównych zasad opisanych w RODO, czyli zasady rozliczalności.

Przedszkole prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje

sposób, w jaki wykorzystuje dane osobowe. Rejestr czynności stanowi podstawowe narzędzie do rozliczenia wszystkich obowiązków ochrony danych.

W Rejestrze czynności, dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb Rejestru, odnotowuje się co najmniej:

1. Określenie czynności przetwarzania/nazwa zbioru;
2. Właściciel aktywów;
3. Cel przetwarzania;
4. Kategorie osób, których dane dotyczą;
5. Kategorie danych osobowych;
6. Podstawa prawna;
7. Źródło pozyskania danych;
8. Planowany termin usunięcia kategorii danych (lub kryterium określenia terminu);
9. Nazwa współadministratora i dane kontaktowe (jeśli dotyczy);
10. Nazwa podmiotu przetwarzającego i dane kontaktowe;
11. Kategorie odbiorców (innych niż podmiot przetwarzający);
12. Sposób przetwarzania/nazwa programu;
13. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie (art. 32 ust. 1 RODO);
14. Ocena skutków dla ochrony danych;
15. Transfer do kraju trzeciego lub organizacji międzynarodowej;
16. Ewentualne środki zabezpieczeń poza EOG

W przypadku gdy Administrator danych występuje także w roli Podmiotu Przetwarzającego, na mocy umowy o powierzeniu przetwarzania danych osobowych, prowadzi on Rejestr Kategorii Czynności przetwarzania danych osobowych.

III.ZASADA ROZLICZALNOŚCI

W ramach realizacji zasady rozliczalności Administrator danych osobowych jest w stanie wykazać, iż przetwarzane przez niego dane są:

1. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub histo-

rycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 Rozporządzenia za niezgodne z pierwotnymi celami („ograniczenie celu”);

3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
4. prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
5. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 Rozporządzenia, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);
6. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

III.ZGODNOŚĆ PRZETWARZANIA DANYCH OSOBOWYCH Z PRAWEM

Administrator zgodnie z zasada rozliczalności zapewnia, by dane osobowe przetwarzane były zgodnie z prawem, w sposób rzetelny i przejrzysty. Dane osobowe przetwarzane są w zakresie niezbędnym dla realizacji celów tego przetwarzania. Cele przetwarzania określane są w sposób wyraźny i konkretny, dalsze zaś przetwarzanie w sposób niezgodny z tymi celami jest zabronione za wyjątkiem przypadków wskazanych w przepisach obowiązującego prawa, bądź po uzyskaniu zgody na przetwarzanie danych osobowych dla nowych celów. Dane osobowe są aktualne i prawidłowe i w razie potrzeby uaktualniane.

Dane osobowe przechowywane są przez oznaczony czas niezbędny dla zapewnienia realizacji celów przetwarzania lub do czasu przedawnienia ewentualnych roszczeń.

Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel administratora) Publiczne Przedszkole nr 1 w Pile

określa podstawę w czytelny sposób, gdy jest to potrzebne np. w przypadku zgody wskazując na jej zakres, gdy podstawą jest przepis prawa – wskazując na konkretny przepis, dla uzasadnionego celu Administratora– wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.

Administrator danych osobowych zapewnia wykonanie wobec osób, których dane dotyczą obowiązku informacyjnego zgodnie z art. 13 (w przypadku pozyskania danych od osoby, której dane dotyczą) i 14 (w przypadku pozyskania danych nie od osoby, której dane dotyczą) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 („RODO"), wskazując prawa przysługujące tym osobom w tym: prawa dostępu do danych osobowych, sprostowania, usunięcia tzw. prawo do „bycia zapomnianym", ograniczenia przetwarzania, wniesienia sprzeciwu czy cofnięcia zgody na przetwarzanie danych osobowych. Osoby te informuje się również o tym, kto jest administratorem ich danych osobowych, o powołanym Inspektorze Ochrony Danych oraz jego danych kontaktowych. Administratora danych nie obejmuje obowiązek informowania osoby, której dane dotyczą w przypadku, gdy dane te muszą zostać objęte tajemnicą zawodową.

Wskazane wyżej informacje Administrator podaje do wiadomości osoby, której dane dotyczą:

1. w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
2. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą;
3. jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

Wzory stosowanych przez administratora klauzul obowiązku informacyjnego stanowi załącznik nr 3 do Zarządzenia.

Przy powierzaniu przetwarzania danych osobowych w imieniu Administratora, dokonuje on wyboru wyłącznie takich podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. W tym celu Administrator zawiera z podmiotami przetwarzającymi stosowne umowy powierzenia przetwarzania danych osobowych (art. 28 RODO). Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik nr 3 do Zarządzenia.

III.ANALIZA RYZYKA I OCENA SKUTKÓW DLA OCHRONY DANYCH

Administrator danych osobowych uwzględnia ryzyko naruszenia praw i wolności osób fizycznych, których dane dotyczą, wdrażając odpowiednie środki techniczne i organizacyjne celem zapewnienia

stopnia bezpieczeństwa odpowiadającego temu ryzyku. Zarządzanie ryzykiem w Publicznym Przedszkolu Nr 1 w Pile odbywa się zgodnie z przyjętymi zasadami i z uwzględnieniem prawdopodobieństwa wystąpienia zagrożenia oraz jego skutków.

Administrator we współpracy z Inspektorem Ochrony Danych przeprowadza analizę ryzyka dla poszczególnych operacji przetwarzania danych w zakresie aktywów biorących udział w przetwarzaniu danych lub dla zbioru danych osobowych lub grupy zbiorów charakteryzujących się podobieństwem celów i sposobów przetwarzania.

Celem zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń dokonuje się analizy ryzyka naruszenia praw i wolności osób, których dane dotyczą.

W przypadku, gdy konieczne jest dokonanie oceny skutków dla ochrony danych osobowych podejmuje się następujące czynności:

1. sporządzenie opisu planowanych operacji przetwarzania danych osobowych z określeniem celu przetwarzania dla każdej z nich;
2. diagnoza zagrożeń związanych z wykorzystaniem aktywów stosowanych w procesie przetwarzania danych osobowych;
3. ocena poziomu ryzyka, zgodnie z przyjętymi w Przedszkolu zasadami;
4. sporządzenie macierzy ze wskazaniem istotności ryzyka;
5. przygotowanie raportu i wdrożenie planu naprawczego przewidującego środki techniczne, organizacyjne i informatyczne odpowiednie dla ryzyk, których stopień przekracza poziom średni.

III. INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH

Instrukcja określa katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych w Publicznym Przedszkolu Nr 1 w Pile oraz w jasny sposób pokazuje jak należy na nie reagować. Instrukcja na ma celu zminimalizowanie skutków wystąpienia naruszenia zasad ochrony danych osobowych oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
Każde naruszenie bądź podejrzenie naruszenia zasad ochrony danych osobowych powinno być niezwłocznie zgłaszane bezpośredniemu przełożonemu, Inspektorowi Ochrony Danych Osobowych w Przedszkolu bądź bezpośrednio do Administratora danych osobowych.
Za naruszenie lub próbę naruszenia zasad przetwarzania danych osobowych uznaje się:

1. nieodpowiednie zabezpieczenie pomieszczeń, urządzeń lub dokumentów;
2. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
3. naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe;
4. uszkodzenie, utrata, zmiana, lub nieuprawnione kopiowanie danych osobowych;
5. udostępnienie lub możliwość udostępnienia danych osobowych osobom nieuprawnionym;
6. nieprzestrzeganie obowiązku ochrony przetwarzanych danych osobowych;
7. niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczeń;
8. przetwarzanie danych osobowych bez upoważnienia;
9. przetwarzanie danych osobowych niezgodnie z ich zakresem lub celem zebrania;
10. przetwarzanie danych osobowych poza obszarem przetwarzania danych osobowych bez wiedzy i zgody Administratora;
11. naruszenie praw osób, których dane dotyczą;
12. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie na klucz pomieszczeń, szaf, biurek).

Typowymi incydentami bezpieczeństwa danych osobowych nazwać można:

1. wszystkie nieprzewidziane zdarzenia losowe w obszarze przetwarzania danych osobowych, takie jak: pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności;
2. wszystkie zdarzenia losowe dotyczące sprzętów, takie jak: awarie serwera, komputerów, twardych dysków, pendrive, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych, brak możliwości zalogowania się do systemu, zmiana wyglądu pulpitu komputera);
3. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

W poniższych tabelach opisano konkretne sytuacje i proponowany sposób postępowania z naruszeniami.

- **naruszenia ochrony danych osobowych przez osoby zatrudnione przy przetwarzaniu danych**

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA

W ZAKRESIE WIEDZY	
Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić przełożonego.
Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	
Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.	
W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA	
Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport
Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport.
Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić przełożonego. Sporządzić raport.
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić przełożonego. Sporządzić raport.
Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać informatyka w celu odinstalowania programów. Sporządzić raport.
Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. Sporządzić raport.
Odczytywanie nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność o szkodliwości takiego działania. Wezwać informatyka w celu wykonania kontroli antywirusowej. Sporządzić raport.
W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	
Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Sporządzić raport.
Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych.	Powiadomić przełożonych w celu poprawienia zabezpieczeń. Sporządzić raport.

Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport.
Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane - sporządzić raport.
Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonego. Sporządzić raport.
Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić przełożonego. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć pomieszczenie. Powiadomić przełożonych. Sporządzić raport.
Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych. Sporządzić raport.
Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakikolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić przełożonego. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	
Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub oka-	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość.

blowaniu sieci komputerowej w miejscach publicznych.	Powiadomić informatyka i przełożonego. Sporządzić raport.
Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych.	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić informatyka. Sporządzić raport.

- **zjawisk świadczących o możliwości naruszenia ochrony danych osobowych**

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić informatyka. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Powiadomić niezwłocznie informatyka. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	
Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	
Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	
Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Postępować zgodnie z właściwymi przepisami. Powiadomić przełożonego. Sporządzić raport.

- **naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem**

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Powiadomić informatyka oraz przełożonego. Sporządzić raport.
Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	

Każdorazowo po otrzymaniu informacji o zaistnieniu lub możliwości zaistnienia naruszenia zasad ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło

spowodować ryzyko naruszenia praw lub wolności osoby fizycznej. Czynności te ujęte są w raporcie z naruszenia bezpieczeństwa zasad ochrony danych osobowych, który stanowi załącznik nr 3 do Zarządzenia. W przypadku stwierdzenia wystąpienia naruszenia ochrony danych osobowych, Administrator lub IOD prowadzi postępowanie wyjaśniające w toku, którego:

1. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
2. proponuje ewentualne działania zaradcze;
3. zaleca szereg działań mających na celu przywrócenia prawidłowego działania organizacji po wystąpieniu incydentu;
4. rekomenduje działania mające na celu zapobieganie podobnym incydentom w przyszłości lub zmniejszenie strat w momencie ich zaistnienia.

Administrator ewidencjonuje wszelkie powyższe naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, ich skutki oraz podjęte działania zaradcze w formularzu rejestracji incydentów, stanowiącym załącznik nr 3 do Zarządzenia.

W każdej sytuacji, w której Administrator stwierdził możliwość wystąpienia ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, zgłasza fakt naruszenia ochrony danych osobowych do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych bez zbędnej zwłoki, jednakże nie później niż w ciągu 72 godzin od momentu stwierdzenia naruszenia. Zgłoszenia naruszenia dokonuje się elektronicznie za pomocą odpowiedniego formularza dostępnego na stronie internetowej Urzędu Ochrony Danych Osobowych: uodo.gov.pl. Formularz należy wypełnić a następnie załączyć do pisma ogólnego dostępnego na platformie biznes.gov.pl bądź wysłać przez elektroniczną skrzynkę podawczą ePUAP: /UODO/SkrytkaESP

Jeżeli zaistniałe ryzyko naruszenia ochrony danych osobowych, jest wysokie dla osoby, której dane dotyczą, Administrator informuje ją, wskazując jednocześnie w jaki sposób zagrożona osoba może sama się chronić.
Zabrania się świadomego wywoływania incydentów przez wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w Publicznym Przedszkolu nr 1 w Pile.

III. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych w celu zapewnienia ochrony danych osobowych stosuje się odpowiednie rozwiązania organizacyjne i techniczne

1. Przedszkole przetwarza dane osobowe zgodnie z przepisami prawa w tym RODO oraz Ustawa o ochronie danych osobowych z dnia 10 maja 2018 roku oraz wewnętrznymi politykami i

procedurami.

2.Budynek Przedszkola objęty jest systemem kontroli dostępu, w tym sygnalizacji włamania.

3.Elektroniczne systemy monitoringu pozwalają na kontrole ruchu osób i informują Firmę Ochrony Mienia „Asecura" o przypadkach nieautoryzowanego wejścia.

4.Każdy pracownik przedszkola przed dopuszczeniem do przetwarzania danych osobowych zobowiązany jest do zapoznania się oraz stosowania przepisów o ochronie danych osobowych i instrukcji wewnątrz przedszkolnych.

5.Pomieszczenia w których przetwarzane są dane osobowe zamykane są na klucz, jeżeli nie przebywa w nich osoba uprawniona.

6.Monitory ustawione są w sposób uniemożliwiający oglądanie ekranu z miejsc ogólnodostępnych.

7.Bieżące naprawy komputera dokonywane są w obecności użytkownika systemu.

8.Administrator sieci informatycznej jest osobą uprawnioną do nadzoru instalowania i usuwania oprogramowania systemowego i narzędziowego. Dopuszcza się instalowanie tylko legalnie pozyskanych programów niezbędnych do wykonywania ustalonych i statutowych zadań przedszkola i posiadających ważną licencję użytkowania.

9.Wykorzystywanie akt i dokumentów, zawierających dane osobowe (dzienniki zajęć), do pracy w domu jest kategorycznie zabronione.

10.Dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie lub usunięcie danych programem trwale usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone.

11.Po wykorzystaniu wydruki, zawierające dane osobowe, należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora.

12.Ważnym elementem Polityki Ochrony Danych jest Rejestr Czynności Przetwarzania Danych Osobowych (RCPD). Identyfikuje on wszystkie procesy dotyczące danych osobowych zachodzące na wszystkich zbiorach, pozwala na kontrolę nad tymi procesami oraz systemami używanymi do ich realizacji. RCPD stanowi formę dokumentowania czynności przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację jednej z głównych zasad opisanych w RODO, czyli zasady rozliczalności.

13.Administrator zgodnie z zasadą rozliczalności zapewnia, by dane osobowe przetwarzane były zgodnie z prawem, w sposób rzetelny i przejrzysty. Dane osobowe przetwarzane są w zakresie niezbędnym dla realizacji celów tego przetwarzania. Cele przetwarzania określane są w sposób wyraźny i konkretny, dalsze zaś przetwarzanie w sposób niezgodny z tymi celami jest zabronione

za wyjątkiem przypadków wskazanych w przepisach obowiązującego prawa, bądź po uzyskaniu zgody na przetwarzanie danych osobowych dla nowych celów. Dane osobowe są aktualne i prawidłowe i w razie potrzeby uaktualniane.

14. Administrator danych osobowych zapewnia realizację wobec osób, których dane dotyczą obowiązku informacyjnego zgodnie z art. 13 (w przypadku pozyskania danych od osoby, której dane dotyczą) i 14 (w przypadku pozyskania danych nie od osoby, której dane dotyczą) z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 („RODO"), wskazując prawa przysługujące tym osobom w tym: prawa dostępu do danych osobowych, sprostowania, usunięcia tzw. prawo do „bycia zapomnianym", ograniczenia przetwarzania, wniesienia sprzeciwu czy cofnięcia zgody na przetwarzanie danych osobowych. Osoby te informuje się również o tym, kto jest administratorem ich danych osobowych, o powołanym Inspektorze Ochrony Danych oraz jego danych kontaktowych.
15. Pocztą elektroniczną można przesyłać tylko jednostkowe dane, a nie całe bazy lub szerokie z nich wypisy i tylko w postaci zaszyfrowanej. Chroni to przesyłane dane przed „przesłuchami" na liniach teletransmisyjnych oraz przed przypadkowym rozproszeniem ich w Internecie przed atakami z sieci zewnętrznej wszystkie komputery administratora danych chronione są środkami dobranymi przez inspektora ochrony danych. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora danych oraz umożliwić mu monitorowanie i aktualizację środków (urządzeń, programów) bezpieczeństwa.
16. Administrator systemu informatycznego dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.
17. Osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych, zgodnie z zakresem upoważnienia do ich przetwarzania. Administrator systemu informatycznego przydziela pracownikowi upoważnionemu do przetwarzania danych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem.
18. Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń inspektora ochrony danych.
19. Operacje za pośrednictwem rachunku bankowego administratora danych może wykonywać osoba zgodnie z karta wzorów podpisów.
20. W przedszkolu używa się komputery przenośne (laptopy) do przetwarzania danych osobowych.

21.Odpowiedzialnym za monitorowanie dostępu do systemu i jego użycia jest administrator sieci.

22.Z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez administratora danych, w której usunięto dane osobowe.

23.Udostępnianie danych osobowych policji, służbie miejskiej i sądom może nastąpić w związku z prowadzonym przez nie postępowaniem a udostępnianie danych osobowych funkcjonariuszom policji może nastąpić tylko po przedłożeniu wniosku o przekazanie lub udostępnienie informacji. Wniosek ten powinien mieć formę pisemną.

24.Osoba udostępniająca dane osobowe, jest obowiązana zażądać od policjanta pokwitowania pobrania dokumentów zawierających informacje przekazane na podstawie pisemnego wniosku albo potwierdzenia faktu uzyskania wglądu w treść informacji.

25.Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.

26.Niezależnie od rozwiązania stosunku pracy osoby, popełniające przestępstwo, będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51 i 52. ustawy oraz art. 266. Kodeksu karnego.

III.Przeglądy polityki bezpieczeństwa i audyty systemu

Polityka bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych inspektor ochrony danych może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.

Inspektor ochrony danych analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:

1.zmian w budowie systemu informatycznego,

2.zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych,

3.zmian w obowiązującym prawie.

Inspektor Ochrony Danych po uzgodnieniu z dyrektorem przedszkola może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z administratorem systemu. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym zarówno przez inspektora ochrony danych jak i dyrektora. Dyrektor przedszkola, biorąc pod uwagę wnioski inspektora ochrony danych, może zlecić przeprowadzenie audytu zewnętrznego przez

wyspecjalizowany podmiot.

III.XI. POSTANOWIENIA KOŃCOWE

1.Każda osoba, upoważniona do przetwarzania danych osobowych, zobowiązania jest do zapoznania się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści (załącznik nr 2 do zarządzenia).

2.Niezastosowanie się do postanowień niniejszego dokumentu i naruszenie procedur ochrony danych jest traktowane jako ciężkie naruszenie obowiązków służbowych, skutkujące poważnymi konsekwencjami prawnymi włącznie z rozwiązaniem stosunku pracy na podstawie art. 52. Kodeksu pracy.

3.Polityka bezpieczeństwa, wchodzi w życie z dniem 11 grudnia 2018 r.

....

(miejscowość, data) (podpis i pieczęć dyrektora)

Instrukcja zarządzania systemami informatycznymi w Publicznym Przedszkolu Nr 1 w Pile

Załącznik Nr 2
do zarządzenia
Dyrektora Publicznego Przedszkola Nr 1 w Pile
z dnia 11 grudnia 2018 r.

Instrukcja zarządzania systemami informatycznymi
w Publicznym Przedszkolu Nr 1 w Pile

I. POSTANOWIENIA WSTĘPNE

1. W celu zapewnienia bezpieczeństwa informacji wprowadza się szczegółowe zasady zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, a także stosowanymi do korzystania z zasobów Internetu.
2. Wszystkie systemy informatyczne działające w przedszkolu, które zawierają dane osobowe podlegają ochronie na mocy 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 Instrukcja jest dokumentem powiązanym z „Polityką bezpieczeństwa w Publicznym Przedszkolu nr 1 w Pile i stanowi dokumentację ochrony danych osobowych.
3. Niniejsza instrukcja znajduje zastosowanie do systemów informatycznych, stosowanych w przedszkolu, w których są przetwarzane dane osobowe.
4. Instrukcja jest przeglądana i w razie potrzeby uaktualniana przez administratora danych osobowych lub upoważnioną przez niego osobę.
5. Dyrektor przedszkola jest odpowiedzialny za ochronę danych osobowych. W celu realizacji tego zadania wyznacza osobę pełniącą funkcje inspektora ochrony danych.

I. Definicje

Ilekroć w instrukcji jest mowa o:

1. **Administratorze danych** – rozumie się przez to Publiczne Przedszkole nr 1, reprezentowane przez Dyrektora, decydującego o celach i środkach przetwarzania danych,
2. **Inspektorze ochrony danych** – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków inspektora ochrony danych,
3. **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,
4. **identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w

systemie informatycznym,

5. **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osobę upoważnioną do przetwarzania danych; osobę, której powierzono przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,
6. **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to pracownika przedszkola, który upoważniony został do przetwarzania danych osobowych przez dyrektora przedszkola na piśmie,
7. **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
8. **serwisancie** – rozumie się przez to firmę lub pracownika firmy, zajmującej się instalacją, naprawą i konserwacją sprzętu komputerowego,
9. **sieci publicznej** – rozumie się przez to sieć telekomunikacyjną, wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych,
10. **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
11. **przedszkole** – rozumie się przez to Publiczne Przedszkole nr 1 w Pile,
12. **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,
13. **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
14. **użytkowniku** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

I. Nadawanie i rejestrowanie (wyrejestrowanie) uprawnień do przetwarzania danych w systemie informatycznym.

1. Nadawanie i rejestrowanie uprawnień.

1.1. Dostęp do systemu informatycznego, służącego do przetwarzania danych osobowych, może uzyskać wyłącznie osoba upoważniona do przetwarzania danych osobowych, zarejestrowana jako użytkownik w tym systemie przez dyrektora przedszkola lub uprawnioną przez niego osobę.

1.2. Rejestracja użytkownika, o którym jest mowa w pkt. 1.1., polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do bazy użytkowników systemu.

2. **Wyrejestrowanie uprawnień.**

2.1. Wyrejestrowanie użytkownika systemu informatycznego dokonuje dyrektor przedszkola lub upoważniona przez niego osoba.

2.2. Wyrejestrowanie, o którym jest mowa w pkt. 2.1., może mieć charakter czasowy lub trwały.

2.3. Wyrejestrowanie następuje przez:

2.3.1. zablokowanie konta użytkownika do czasu ustania przyczyny, uzasadniającej blokadę (wyrejestrowanie czasowe),

2.3.2. usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

2.4. Czasowe wyrejestrowanie użytkownika z systemu musi nastąpić w razie:

2.4.1. nieobecności użytkownika w pracy, trwającej dłużej niż 21 dni kalendarzowych,

2.4.2. zawieszenia w pełnieniu obowiązków służbowych.

2.5. Przyczyną czasowego wyrejestrowania użytkownika z systemu informatycznego może być:

2.5.1. wypowiedzenie umowy o pracę,

2.5.2. wszczęcie postępowania dyscyplinarnego.

2.6. Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

I. Metody i środki uwierzytelniania

1. Każdy użytkownik systemu informatycznego otrzymuje identyfikator i hasło.

2. Identyfikator składa się z co najmniej ośmiu znaków. W identyfikatorze pomija się polskie znaki diakrytyczne.

3. Hasło użytkownika powinno składać się z unikalnego zestawu, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani jego imieniem lub nazwiskiem.

4. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.

5. Zmiana haseł w systemie następuje nie rzadziej niż co 30 dni.

I. Procedury

1. **Procedury rozpoczęcia i zakończenia pracy przeznaczone dla użytkowników systemu.**

1.1. Przed uruchomieniem komputera należy sprawdzić czy nie zostały do niego podłączone niezidentyfikowane urządzenia.

1.2. Rozpoczynając pracę, użytkownik włącza komputer i podaje hasło w celu uruchomienia

systemu operacyjnego.

1.3. Użytkownik rozpoczynając pracę w sieci, musi podać przydzieloną mu nazwę użytkownika sieci i hasło dostępu. Dla zapewnienia bezpieczeństwa sieci teleinformatycznej hasło powinno być zmieniane cyklicznie, przynajmniej raz na kwartał, a także każdorazowo po zaistnieniu uzasadnionego podejrzenia o ujawnieniu hasła osobie nieuprawnionej.

1.4. Uruchomienie programów następuje po podaniu identyfikatora użytkownika i hasła.

1.5. Identyfikator użytkownika jest nadawany przez administratora systemu, który może również przydzielić użytkownikowi pierwsze hasło. W takim przypadku użytkownik przy pierwszym logowaniu powinien zmienić hasło.

1.6. W przypadku, kiedy użytkownik musi opuścić stanowisko pracy, powinien wyjść z programu, włączyć wygaszasz ekranu chroniony hasłem albo wylogować komputer z sieci, aby uniemożliwić nieuprawnionym osobom przeglądanie oraz ewentualne modyfikowanie lub wprowadzenie danych.

1.7. Na stanowiskach pracujących pod systemem WINDOWS powinien być włączany wygaszacz ekranu jeżeli nie są wykonywane żadne operacje –uniemożliwia to dalszą pracę bez podaniu hasła. W uzasadnionych przypadkach dyrektor przedszkola może wyrazić zgodę na wyłączenie opcji wygaszacza ekranu.

1.8. Po zakończeniu pracy użytkownik zamyka programy oraz system operacyjny, a następnie wyłącza komputer.

2. **Hasło**

2.1. W haśle nie należy stosować popularnych nazw komputerowych, nazw znanych postaci bajkowych, literackich, filmowych. Hasło nie powinno kojarzyć się z użytkownikiem ani jego otoczeniem (imiona, nazwiska, adresy, daty itp.)

2.2. Hasło objęte jest tajemnicą i dlatego nie może być udostępniane osobom trzecim ani przechowywane w dostępnym miejscu.

2.3. Hasło zmieniane jest cyklicznie, przynajmniej raz na 30 dni.

3. **Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności**

3.1. Ewidencje osób zatrudnionych przy komputerowym przetwarzaniu danych osobowych prowadzi administrator danych osobowych lub wyznaczony przez niego pracownik.

3.2. Dyrektor przedszkola wypełnia upoważnienie, które zawiera: imię i nazwisko pracownika, prawa dostępu, datę – od kiedy obowiązują.

3.3. Administrator sieci informatycznej w uzgodnieniu z pracownikiem, nadaje pracownikowi

identyfikator, uprawnienia użytkownika oraz ustala z nim hasło dostępu.

3.4. Użytkownik może mieć tylko jeden identyfikator w systemie. Identyfikator raz przydzielony jednemu użytkownikowi, nie może być powtórnie nadany drugiemu użytkownikowi.

3.5. W przypadku, gdy użytkownik stracił prawa do wykonywania dotychczasowych zadań, to jego upoważnienie wygasa i zostaje on usunięty z rejestru użytkowników systemu; kasowane są również nadane mu wcześniej prawa dostępu do systemu i katalogów sieciowych.

4. **Sposób zabezpieczenia systemu teleinformatycznego przed oprogramowaniem złośliwym**

4.1. Stosowanie oprogramowania antywirusowego.

4.2. Dbałość o aktualizację wykorzystywanej wersji oprogramowania antywirusowego.

4.3. Tylko osoby upoważnione przez dyrektora przedszkola mogą wprowadzać do sieci dane z zewnętrznych nośników informacji.

5. **Procedury i zasady obowiązujące przy pracy na stanowisku komputerowym**

5.1. Zalogowanie do systemu wymaga podania hasła.

5.2. Użytkownik nie może opuszczać stanowiska komputerowego nie zabezpieczając komputera przed nieuprawnionym dostępem do systemu lub programów. Zaleca się stosowanie wylogowania z systemu lub wygaszacz ekranu zabezpieczony hasłem.

5.3. Zabrania się użytkownikom:

5.3.1. Udostępniania stanowisk komputerowych, haseł oraz zasobów informatycznych osobom nieupoważnionym,

5.3.2. Wykorzystywania stanowiska komputerowego w celach innych niż wykonywanie obowiązków związanych z zakresem zadań powierzonych przez przełożonego,

5.3.3. Samowolnego instalowania i używania programów komputerowych oraz przenoszenia sprzętu komputerowego,

5.3.4. Kopiowania programów komputerowych oraz danych przetwarzanych w systemie,

5.3.5. Wynoszenia danych z siedziby przedszkola na nośnikach elektronicznych lub na papierze,

5.3.6. Odklejania naklejek świadczących o legalności oprogramowania oraz plomb zabezpieczających komputer,

5.3.7. Używania elektronicznych nośników informacji podejrzanych o zainfekowanie wirusem. W takim przypadku należy zgłosić się z nośnikiem do administratora systemu.

5.4. Zobowiązuje się pracowników do:

5.4.1. Ustawienia monitorów w sposób uniemożliwiający podgląd zawartości ekranu monitora przez osoby nieupoważnione,

5.4.2. Niszczenia w niszczarkach zbędnych wydruków zawierających dane osobowe,

5.4.3. Przeglądania co najmniej raz dziennie poczty elektronicznej,

5.4.4. Zgłaszania wszystkich nieprawidłowości w działaniu sprzętu i oprogramowania oraz prób nieautoryzowanego naruszenia zabezpieczeń do administratora systemu i inspektora ochrony danych oraz powiadamiania o tych zdarzeniach dyrektora przedszkola.

6. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

6.1. Aktualizacja baz danych i oprogramowania przeprowadzana jest przez administratora sieci informatycznej.

6.2. Konserwacja sprzętu komputerowego przeprowadzana jest przez administratora sieci informatycznej lub firmę zewnętrzną.

6.3. W przypadku awarii sprzętu, na którym znajdują się dane osobowe w zależności od uszkodzenia następuje:

6.3.1. naprawa na miejscu pod nadzorem administratora danych,

6.3.2. demontowanie dysku i zabezpieczenie go w szafie metalowej w biurze na czas naprawy,

6.3.3. przegrywanie danych przez administratora danych na inny nośnik i usunięcie danych z przekazywanego do naprawy sprzętu.

6.4. W przypadku przekazania komputerów innemu użytkownikowi lub jednostce organizacyjnej, dane z dysków twardych są usuwane na zlecenie administratora danych przez administratora sieci informatycznej w sposób uniemożliwiający ich odtworzenie.

6.5. W przypadku złomowania sprzętu komputerowego, nośniki informacji (dyski twarde) powinny być fizycznie niszczone przez komisję powołaną do realizacji tego zadania (z udziałem administratora danych).

7. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

Kopie zbiorów danych dokonywane są w placówce, na serwerze wewnętrznym na bieżąco.

8. Procedury transportu przesyłek zawierających dane osobowe, przesyłek wartościowych lub transportu innych ważnych danych

8.1. Instrukcja obejmuje w szczególności transport przesyłek zawierających: nośniki z danymi osobowymi, wydruki przelewów, kopie baz danych i programów wykonane przez administratora systemu.
8.2. Przez transport należy rozumieć przenoszenie lub przewożenie przesyłek.
8.3. Transportu przesyłek dokonują pracownicy wyznaczeni przez dyrektora przedszkola.
8.4. Transport przesyłek z danymi osobowymi lub innymi materiałami, może być realizowany pieszo lub pojazdem.
8.5. Transport kopii baz danych i programów musi być każdorazowo uzgodniony z dyrektorem przedszkola.

I. Poziom bezpieczeństwa

Uwzględniając kategorie danych osobowych oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie informatycznym, połączonym z siecią publiczną, wprowadza się wysoki poziom bezpieczeństwa.

II. Stosowane środki bezpieczeństwa

1. Zgodnie z treścią art. 32 RODO w przedszkolu stosuje się środki bezpieczeństwa na poziomie wysokim.
2. W przedszkolu stosuje się następujące środki bezpieczeństwa:

1.1. Zabezpieczenie obszaru, w którym przetwarzane są dane osobowe, przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.
1.2. Przebywanie osób nieuprawnionych, jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
1.3. Stosowane są mechanizmy kontroli dostępu do danych.
1.4. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie jest przydzielany innej osobie.
1.5. W przypadku, gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej, niż co 90 dni. Hasło składa się, co najmniej z 8 znaków. Hasło to zawiera małe i wielkie litery oraz cyfry i znaki specjalne.
1.6. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych na serwerze wewnętrznym oraz programów, służących do przetwarzania danych osobowych.
1.7. Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.
1.8. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe,

przeznaczone do:

1.8.1. likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

1.8.2. przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie.

1.8.3. naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej do przetwarzania danych osobowych przez administratora danych.

1.9. Urządzenia i nośniki, zawierające dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

1.10. Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

I. Postanowienia końcowe

1. Osobą odpowiedzialną za przegląd przestrzegania instrukcji, przegląd jej aktualności oraz aktualizację, a także nadawanie praw dostępu do systemu informatycznego jest inspektor ochrony danych lub inna osoba upoważniona przez administratora danych.
2. W sprawach nieokreślonych niniejszą instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją
4. Niezastosowanie się do procedur określonych w niniejszej instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52. kodeksu pracy.
5. Niniejsza instrukcja wchodzi w życie z dniem podjęcia.

W przypadku stwierdzenia nie stosowania przez pracowników niniejszej Instrukcji, administrator systemu na polecenie dyrektora przedszkola blokuje użytkownikowi prawo wejścia do sieci i korzystania z jej zasobów. Odblokowanie użytkownika w sieci następuje również na polecenie dyrektora przedszkola.

....

(miejscowość, data) (podpis i pieczęć dyrektora)

WYKAZ
PROGRAMÓW KOMPUTEROWYCH
STOSOWANYCH W

PUBLICZNYM PRZEDSZKOLU NR 1 W PILE

1.**Bankowe konto internetowe** w PKO – IPKO BIZNES umożliwia dostęp do następujących usług bankowych:

1.1.sporządzanie przelewów – w tym składki ZUS i dla urzędów skarbowych – zadania te realizuje CUW

1.2.sprawdzanie stanu rachunków – zadania realizuje CUW i Publiczne Przedszkole Nr 1

2.**Arkusz organizacji przedszkola** AOS – Vulcan

3.**Program naboru – Poznańskie Centrum Komputerowo-Sieciowe**

....
(miejscowość, data) (podpis i pieczęć dyrektora)

Załącznik Nr 3
do zarządzenia
Dyrektora Publicznego Przedszkola Nr 1w Pile
z dnia 11 grudnia 2018 r.

Dokumentowanie przetwarzania danych osobowych - wykaz wzorów obowiązujących w Publicznym Przedszkolu Nr 1 w Pile

1.KLAUZULA ZGODY I OBOWIĄZKU INFORMACYJNEGO DO FORMULARZA REKRUTACJI DZIECI

Wyrażam zgodę na przetwarzanie danych osobowych podanych w niniejszym formularzu w celu realizacji statutowych zadań dydaktycznych, opiekuńczych i wychowawczych wobec dziecka, którego dane dotyczą.
Zgodnie z art. 13 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 (4.5.2016 L 119/38 Dziennik Urzędowy Unii Europejskiej PL)
przyjmuję do wiadomości, że:
1. Administratorem podanych przeze mnie danych osobowych jest Publiczne Przedszkole Nr 1 w Pile, ul. dr. Franciszka Witaszka 4 , e-mail: przedszkolenr1@asta-net.com.pl .
2. Inspektorem ochrony danych w Publicznym Przedszkolu Nr 12 jest Dawid Nogaj e mail: inspektor@bezpieczne-dane.eu
3. Podane dane osobowe będą na podstawie niniejszej zgody przetwarzane przez administratora przez okres rekrutacji na rok szkolny 2018/2019 i realizacji działalności dydaktyczno-wychowawczo-opiekuńczej wobec dziecka, którego dane dotyczą.
4. Dane nie będą udostępniane podmiotom innym niż upoważnione na podstawie stosownych przepisów prawa.
5. Przysługuje mi prawo żądania dostępu do podanych przeze mnie danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
6. Ponadto, przysługuje mi prawo do cofnięcia wyrażonej zgody w dowolnym momencie. Powyższe nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie wyrażonej przeze mnie zgody przed jej cofnięciem.
7. Dodatkowo, przysługuje mi prawo do wniesienia skargi do organu nadzorczego jeżeli uznam, że podane przeze mnie dane osobowe przetwarzane są niezgodnie z przepisami obowiązującego prawa.
8. Podanie przeze mnie danych osobowych jest dobrowolne, przy czym niezbędne do przeprowadzenia procesu rekrutacji do Publicznego Przedszkola Nr 1 i prowadzenia działalności dydaktyczno-wychowawczo-opiekuńczej wobec dziecka, którego dane dotyczą, na podstawie przepisów Ustawy – Prawo oświatowe z dn. 14 grudnia 2016 r. (Dz. U. z 2017 r., poz. 59 oraz Ustawy o systemie oświaty z dnia 7 września 1991 r. (Dz. U. z 2017 r., poz. 2198).

9. Dane nie będą przetwarzane w sposób zautomatyzowany.”

……

(czytelny podpis osoby składającej oświadczenie)

2.KLAUZULA OBOWIĄZKU INFORMACYJNEGO DLA RODZICÓW/OPIEKUNÓW DZIECI UCZĘSZCZAJĄCYCH

Zgodnie z art. 13 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 (4.5.2016 L 119/38 Dziennik Urzędowy Unii Europejskiej PL)
informuję, że:

1. Administratorem podanych przez Pana/Panią danych osobowych jest Publiczne Przedszkole Nr 1 w Pile, ul.dr. Franciszka Witaszka 4 , e-mail: przedszkolenr1@asta-net.com.pl
2. Inspektorem ochrony danych w Publicznym Przedszkolu Nr 1 jest Dawid Nogaj e mail: inspektor@bezpieczne-dane.eu
3. Podane dane osobowe będą przetwarzane przez Publiczne Przedszkole Nr 1 przez okres rekrutacji na rok szkolny 2018/2019 i realizacji działalności dydaktyczno-wychowawczo-opiekuńczej wobec dziecka, którego dane dotyczą.
4. Dane osobowe będą przetwarzane na podstawie art. 6 ust. 1 lit., c w/w ogólnego rozporządzenia o ochronie danych w celu realizacji zadań ustawowych, określonych w Ustawie – Prawo oświatowe z dn. 14 grudnia 2016 r. (Dz. U. z 2017 r., poz. 59).
5. Dane nie będą udostępniane podmiotom innym niż upoważnione na podstawie stosownych przepisów prawa,
6. Przysługuje Pani/Panu prawo żądania dostępu do podanych przeze mnie danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawo do wniesienia sprzeciwu wobec przetwarzania.
7. Dodatkowo, przysługuje Panu/Pani prawo do wniesienia skargi do organu nadzorczego .
8. Podanie przez Pana/Panią danych osobowych jest obowiązkowe, na podstawie przepisów prawa dotyczących rekrutacji do przedszkola i prowadzenia przez przedszkole działalności statutowej.
9. Dane nie będą przetwarzane w sposób zautomatyzowany.

……

(Podpis Administratora danych)

3.KLAUZULA INFORMACYJNA DO REKRUTACJI PRACOWNIKÓW

Zgodnie z art. 13 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 (4.5.2016 L 119/38 Dziennik Urzędowy Unii Europejskiej PL) informuję, że :

1.Administratorem danych osobowych podanych w ogłoszeniu o ofercie pracy jest Publiczne Przedszkole Nr 1 z siedzibą w Pile, ul. dr. Franciszka Witaszka 4

2.Funkcję Inspektora Ochrony Danych pełni Dawid Nogaj , adres e-mail:

inspektor@bezpieczne-dane.eu

3.Dane osobowe będą przetwarzane na podstawie wyrażonej przez Panią/ Pana zgody w celu przeprowadzenia procesu rekrutacji na stanowisko ……..w Publicznym Przedszkolu Nr 1 w Pile

4.Podane dane osobowe nie będą udostępniane podmiotom innym niż upoważnione na podstawie obowiązującego prawa.

5.Dane osobowe będą przechowywane przez okres zatrudnienia i po ustaniu zatrudnienia przez czas wymagany przepisami prawa.

6.Przysługuje Panu/Pani prawo żądania dostępu do podanych danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.

7.Ponadto, przysługuje Panu/Pani prawo do cofnięcia wyrażonej zgody w dowolnym momencie. Powyższe nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie wyrażonej przeze mnie zgody przed jej cofnięciem.

8.Przysługuje Panu/Pani prawo wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych.

9.Podanie danych osobowych jest dobrowolne, lecz niezbędne do przeprowadzenia procesu rekrutacji na w/w stanowisko.

…….

Podpis ADO

Uwaga :

1.Klauzulę zamieszcza się: w ogłoszeniu o ofercie pracy;

2.W ogłoszeniu o naborze na stanowisko kandydat zamieszcza w CV klauzulę o następującej treści:
„Wyrażam zgodę na przetwarzanie podanych przeze mnie danych osobowych przez Publiczne Przedszkole Nr 1 w Pile w celu przeprowadzenia procesu rekrutacji na stanowisko _____” .

1.KLAUZULA INFORMACYJNA DLA PRACOWNIKÓW ZATRUDNIONYCH

Zgodnie z art. 13 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 (4.5.2016 L 119/38 Dziennik Urzędowy Unii Europejskiej PL) informuję, że :

1. Administratorem uzyskanych danych osobowych jest Publiczne Przedszkole Nr 1 z siedzibą w Pile, ul.dr. Franciszka Witaszka 4
2. Funkcję Inspektora Ochrony Danych w Publicznym Przedszkolu Nr 1 pełni Dawid Nogaj , adres e-mail: inspektor@bezpieczne-dane.eu
3. Dane osobowe są przetwarzane w celu związanym z zatrudnieniem.
4. Podane dane osobowe nie będą udostępniane podmiotom innym niż upoważnione na podstawie obowiązującego prawa.
5. Dane osobowe są przechowywane przez okres zatrudnienia i po ustaniu zatrudnienia przez czas wymagany obowiązującymi przepisami prawa.
6. Posiada Pani /Pan prawo do: żądania dostępu do podanych danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
7. Przysługuje Pani/ Panu prawo wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych.
8. Podanie danych osobowych jest obowiązkowe, zgodnie z przepisami Kodeksu Pracy – Ustawa z dnia 26 czerwca 1974 r. (t.j. Dz. U. z 2018 r., poz. 108).

…….
Data i podpis pracownika

Uwaga :
1.Powyższa klauzula dotyczy danych do przetwarzania których uprawnia pracodawcę Kodeks Pracy.
2.Klauzulę dołącza się do kwestionariusza osobowego wypełnianego przez zatrudnionego pracownik i wpina się jako osobny dokument w aktach osobowych

2.UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

(zwana dalej „Umową”)

zawarta dnia …….. r. pomiędzy:

…… *(*dane podmiotu który umowę zawiera)*

zwany w dalszej części umowy **„Podmiotem przetwarzającym”**

reprezentowana przez:

_____

oraz

Publicznym Przedszkolem Nr 12 w Pile, ul. Reja 11 *(*dane podmiotu który umowę zawiera)*

zwany w dalszej części umowy **„Administratorem danych” lub „Administratorem”**

reprezentowana przez:

Dyrektora Barbarę Miszczak

§ 1

Powierzenie przetwarzania danych osobowych

1.Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 unijnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego w dalszej części „Rozporządzeniem”) dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.

2.Podmiot przetwarzający przetwarza powierzone dane osobowe tylko na wyraźne polecenie Administratora danych.

3.Przetwarzanie powierzonych danych osobowych przez Podmiot przetwarzający będzie polegało na przeprowadzeniu badań wstępnych, okresowych i kontrolnych pracowników .

4.Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

5.Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§2

Zakres i cel przetwarzania danych

1.Podmiot przetwarzający będzie przetwarzał powierzone na podstawie umowy dane osobowe *pracowników administratora, w postaci imion i nazwisk, adresu zamieszkania, nr PESEL, stanowiska pracy, itp*.

2.Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu *realizacji umowy nr z dnia …….*
w zakresie prowadzenia badań pracowniczych przez okres trwania umowy

§3

Obowiązki podmiotu przetwarzającego

1.Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.

2.Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.

3.Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.

4.Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.

5.Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

6.W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.

7.Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu 24 h.

§4

Prawo kontroli

1.Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.

2.Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 2 dniowym jego uprzedzeniem.

3.Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni .

4.Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§5

Dalsze powierzenie danych do przetwarzania

1.Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.

2.Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji
z uwagi na ważny interes publiczny.

3.Podwykonawca, o którym mowa w §3 ust. 2 Umowy winien spełniać te same gwarancje i obowiązki, jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.

4.Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 6

Odpowiedzialność Podmiotu przetwarzającego

1.Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.

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

§7

Czas obowiązywania umowy

1.Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *określony w umowie na wykonywanie usługi.*

2.Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem miesięcznego okresu wypowiedzenia.

§8

Rozwiązanie umowy

1.Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:

a)pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;

b)przetwarza dane osobowe w sposób niezgodny z umową;

c)powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

§9

Zasady zachowania poufności

1.Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).

2.Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pi-

semnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§10

Postanowienia końcowe

1.Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.

2.W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.

3.Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy Administratora danych (**lub Podmiotu przetwarzającego w zależności od postanowień stron*).

_____ _____

Administrator danych Podmiot przetwarzający

Piła, dnia …… 2018r

6. OŚWIADCZENIE

o wyrażeniu zgody na wykorzystanie wizerunku dziecka

Oświadczam, że wyrażam zgodę/nie wyrażam zgody na nieodpłatne wykorzystanie wizerunku mojego dziecka …… przez Publiczne Przedszkole Nr 1 w Pile w celu informowania o działalności

dydaktycznej i wychowawczo-opiekuńczej oraz w celu promocji przedszkola na stronie internetowej przedszkola www.przedszkole1nr1pila.pl oraz w TV ASTA i lokalnych dziennikach, np. Tętno Rejonu, Moje 7 dni, Tygodnik Nowy, Tygodnik Pilski

Niniejsza zgoda obejmuje wszelkie formy publikacji, w szczególności plakaty reklamowe, ulotki, drukowane materiały promocyjne, reklamę w gazetach i czasopismach oraz w Internecie itp.

Wizerunek dziecka może być użyty do różnego rodzaju form elektronicznego przetwarzania obrazu, kadrowania i kompozycji, bez obowiązku akceptacji produktu końcowego, lecz nie w formach obraźliwych lub ogólnie uznanych za nieetyczne.

INFORMACJA
Przyjmuję do wiadomości, iż:
1. administratorem podanych przeze mnie danych osobowych jest Publiczne Przedszkole Nr 1 w Pile, ul. dr. Franciszka Witaszka 4
2. funkcję inspektora ochrony danych pełni Dawid Nogaj, adres e-mail: inspektor@bezpieczne-dane.eu
3. podane dane osobowe będą przetwarzane na podstawie niniejszej zgody przez okres pobytu dziecka w przedszkolu.
4. dane nie będą udostępniane podmiotom innym niż upoważnione na podstawie stosownych przepisów prawa,
5. przysługuje mi prawo żądania dostępu do podanych przeze mnie danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
6. Ponadto, przysługuje mi prawo do cofnięcia wyrażonej zgody w dowolnym momencie. Powyższe nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie wyrażonej przeze mnie zgody przed jej cofnięciem.
7. Dodatkowo, przysługuje mi prawo do złożenia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych.
8. Podanie przeze mnie danych osobowych jest dobrowolne.
9. Dane nie będą przetwarzane w sposób zautomatyzowany.

……..……..……..
……

data i podpis rodzica/prawnego opiekuna

7. UPOWAŻNIENIE Nr …….

Piła , dn. ……

WAŻNOŚĆ

od:…….
do:…….

Na podstawie art. 29 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 ochronie danych) (Dz. Urz. UE L 119, s. 1) – dalej RODO

jako Administrator danych osobowych w Publicznym Przedszkolu Nr 1 w Pile, ul. dr. Franciszka Witaszka 4

upoważniam Panią/Pana:

……
(imię i nazwisko)

……
(stanowisko)

do przetwarzania, w ramach wykonywanych obowiązków służbowych, następujących zbiorów danych osobowych:

Nazwa zbioru	Nazwa programu / identyfikator

…….

podpis ADO

1.ZGODA
na przebywanie w obszarze przetwarzania danych osobowych
w Publicznym Przedszkolu Nr 1 w Pile

Piła , dnia .....

WAŻNOŚĆ
od: .....
do: .....

Jako Administrator danych osobowych w Publicznym Przedszkolu Nr 1 w Pile (dalej:

PP - 1), niniejszym wyrażam zgodę Pani / Panu:

……..
(imię i nazwisko)

na przebywanie w pomieszczeniach *: biuro dyrektora, biuro referenta, sale zajęć , gabinet terapii logopedycznej, pedagogicznej, składnica akt, w których przetwarzane są dane osobowe w zakresie niezbędnym do wykonywania obowiązków służbowych.

.....
podpis ADO

*niepotrzebne wykreśl

_____, dnia _____

2.OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Ja, niżej podpisana(y) _____oświadczam, że zapoznano mnie z zasadami ochrony danych osobowych wynikającymi z przepisów obowiązującego prawa, w szczególności ogólnego Rozporządzenia Parlamentu Europejskiego i Rady (UE) o ochronie danych UE 2016/679 z dnia 27.04.2016 r.
Jednocześnie zobowiązuję się do:

1.zachowania w tajemnicy danych osobowych *w sytuacji dostępu do nich podczas wykonywania zleconych czynności w postaci zadań na podstawie zakresu czynności*, *do których miałam (em) dostęp w związku z pełnieniem obowiązków służbowych na stanowisku* _____ w Publicznym Przedszkolu Nr 1 w Pile;

2.nieujawniania danych zawartych w eksploatowanych systemach informatycznych ;

3.nieujawniania danych technologicznych używanych systemów oraz oprogramowania;

4.nieudostępniania osobom nieupoważnionym nośników danych oraz wydruków komputerowych;

5.niekopiowania i nieprzetwarzania danych w sposób inny niż konieczny do wykonywania zadań służbowych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.

_____
podpis oświadczającego

Piła, dnia …….

1.OŚWIADCZENIE O WYRAŻENIU ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

Ja, niżej podpisana(y) _____ *(imię i nazwisko)* niniejszym oświadczam, że wyrażam zgodę na przetwarzanie moich danych osobowych oraz danych osobowych mojego dziecka w postaci *(wskazać kategorie danych)*:
- dane osobowe dziecka i rodziny niezbędne w procesie rekrutacji,
- informacje o stanie zdrowia i rozwoju dziecka niezbędne w celu udzielania pomocy

psychologiczno-pedagogicznej oraz w celu sprawowania właściwej opieki nad dzieckiem,
- dane osobowe na potrzeby rozliczeń finansowych z przedszkolem.
Zgodnie z art. 13 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) (Dz. Urz. UE L 119, s. 1)
zostałam(em) poinformowana (y) i przyjmuję do wiadomości, iż :

1. Administratorem podanych przeze mnie danych osobowych jest Publiczne Przedszkole Nr 1 w Pile, ul. dr. Franciszka 4 (dalej:"PP-1"), e-mail: przedszkolenr1@asta-net.com.pl
2. Inspektorem ochrony danych w PP-1 jest Dawid Nogaj e-mail: inspektor@bezpieczne-dane.eu .
3. Podane dane osobowe będą na podstawie niniejszej zgody przetwarzane przez administratora przez okres uczęszczania dziecka do PP-1.
4. Dane nie będą udostępniane podmiotom innym niż upoważnione na podstawie stosownych przepisów prawa.
5. Przysługuje mi prawo żądania dostępu do podanych przeze mnie danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawo do wniesienia sprzeciwu wobec przetwarzania, a także prawo do przenoszenia danych.
6. Ponadto, przysługuje mi prawo do cofnięcia wyrażonej zgody w dowolnym momencie. Powyższe nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie wyrażonej przeze mnie zgody przed jej cofnięciem.
7. Dodatkowo, przysługuje mi prawo do wniesienia skargi do organu nadzorczego, jeżeli uznam, że podane przeze mnie dane osobowe przetwarzane są niezgodnie z przepisami obowiązującego prawa.
8. Podanie przeze mnie danych osobowych jest dobrowolne, przy czym niezbędne do realizowania zadań statutowych Publicznego Przedszkola Nr 1 w Pile.
9. Dane nie będą przetwarzane w sposób zautomatyzowany.

.....
(czytelny podpis osoby składającej oświadczenie)

2.EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W PUBLICZNYM PRZEDSZKOLU NR 1 W PILE

Nr upoważnienia	Imię i nazwisko osoby upoważnionej	Data		Zakres upoważnienia (zawartość zbioru danych)
		Nadania upoważnienia	Ustania upoważnienia	

3.EWIDENCJA ZGÓD NA PRZEBYWANIE W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH W PUBLICZNYM PRZEDSZKOLU NR 1 W PILE

Nr zgody	Imię i nazwisko osoby	Data		/stanowisko
		wydania zgody	odwołanie	

4.REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH W PUBLICZNYM PRZEDSZKOLU NR 1 W PILE

Lp.	Data naruszenia	Godzina naruszenia	Kategorie osób	Ilość osób	Ilość naruszonych wpisów danych	Nr raportu	Organ nadzorczy	Data zawiadomienia organu	Informacja o zawiadomieniu osób, których dane dotyczą/powód niezawiadomienia
1									

2									
3									
4									
5									
6									
7									
8									

_____

podpis Administratora danych

5.RAPORT
z naruszenia bezpieczeństwa zasad ochrony danych osobowych w Publicznym Przedszkolu Nr 1 w Pile

1. Data zdarzenia: _____ Godzina: _____

Osoba powiadamiająca o zaistniałym zdarzeniu:

_____

(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

Lokalizacja zdarzenia:

_____

(np. nr pokoju, nazwa pomieszczenia)

Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

_____

_____

_____

Możliwe konsekwencje naruszenia ochrony danych osobowych (w tym dla osób, których dane dotyczą):

_____

_____

_____

_____

Przyczyny wystąpienia zdarzenia:

_____

_____

Postępowanie wyjaśniające:

_____

_____

Podjęte działania naprawcze:

_____

_____

_____

(podpis Administratora danych)