Załącznik Nr 1 do Zarządzenia Nr17/2020/20121 Dyrektora Szkoły Podstawowej im. KEN w Brzostku

Polityka ochrony danych osobowych

w Szkole Podstawowej

im. KEN w Brzostku

Spis treści:

§ 1 DEFINICJE

Użyte w niniejszym dokumencie określenia oznaczają:

Administrator danych osobowych (Administrator) –. Szkoła reprezentowana przez dyrektora szkoły

Administrator systemu informatycznego – osoba odpowiedzialna za zapewnienie ciągłości i poprawności działania systemu informatycznego,

Użytkownik – osoba upoważniona przez Administratora danych osobowych do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony indywidualny identyfikator oraz hasło,

dane osobowe (dane) – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,

hasło – ciąg znaków literowych, cyfrowych lub innych, pozwalający na dostęp do systemu informatycznego, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

identyfikator – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do dostępu do systemu informatycznego,

Inspektor ochrony danych osobowych (IOD) – to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/ pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Kontakt z Inspektorem Ochrony Danych tel. 14 68 30 376 w. 22 lub e-mail: iodcuw@brzostek.pl

integralność – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

Podmiot przetwarzający – podmiot, o którym mowa w art. 28 RODO, który dokonuje czynności przetwarzania danych osobowych na zlecenie Administratora danych osobowych,

Polityka – niniejsza Polityka ochrony danych osobowych obowiązująca u Administratora,

poufność – właściwość zapewniająca, że dane osobowe nie są udostępniane nieupoważnionym podmiotom,

profilowanie – dowolne zautomatyzowane przetwarzanie danych osobowych pozwalające ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą – o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa,

przetwarzanie danych osobowych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie i inne, a zwłaszcza te, które wykonuje się w systemach informatycznych,

anonimizacja/pseudonimizacja – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; anonimizacja – w przeciwieństwie do pseudonimizacji – jest procesem nieodwracalnym,

PUODO – Prezes Urzędu Ochrony Danych Osobowych pełniący funkcję organu nadzorczego na terenie Rzeczypospolitej Polskiej w rozumieniu art. 4 pkt 21 w zw. z art. 51 ust. 1 RODO,

RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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),
Naruszenie ochrony danych osobowych (incydent) - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
Zagrożenie – potencjalne naruszenie (potencjalny incydent).
Skutki – rezultaty niepożądanego incydentu (straty w przypadku wystąpienia zagrożenia)
Ryzyko- prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.
zbiór danych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,

2. Podstawa prawna

1. Polityka jest zgodna z następującymi aktami prawnymi:
   a) Konstytucją Rzeczypospolitej Polskiej,
   b) RODO,
   c) Ustawą o ochronie danych osobowych – ustawa z dn. 10 maja 2018r. o ochronie danych osobowych,
   d) przepisami innych aktów prawnych powszechnie obowiązujących w zakresie, w jakim dotyczą ochrony danych osobowych.

Wprowadzenie:

Polityka Bezpieczeństwa Ochrony Danych Osobowych wprowadzona jest na podstawie art. 24 ust. 2, w zw. z art. 5 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, Dz. Urz. UE L 119 z 04.05.2016 r. ze zm.- zwana dalej RODO) Administrator danych osobowych Szkoła Podstawowa im. KEN w Brzostku przyjmuje do stosowania Politykę ochrony danych osobowych.

Polityka ochrony danych służy zapewnieniu ochrony danych osobowych przetwarzanych przez szkołę przez ustanowienie jednolitych reguł postępowania w zakresie przetwarzania danych osobowych.

Zasadniczym celem Polityki jest przyjęcie, wdrożenie i realizacja działań przy zastosowaniu środków technicznych i organizacyjnych, niezbędnych dla zapewnienia poufności, rozliczalności i integralności przetwarzanych danych dając pełne gwarancje ich ochrony.

Polityka bezpieczeństwa realizuje zasadę rozliczalności, o której mowa w art. 5 ust 2 RODO zgodnie z jej treścią Administrator jest odpowiedzialny za przestrzeganie zasad przetwarzania danych osobowych i musi być w stanie wykazać ich przestrzeganie.

Polityka ochrony danych określa sposób prowadzenia oraz zakres dokumentacji odnoszącej się do sposobu przetwarzania danych osobowych.

§ 2 OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

Zgodnie z postanowieniami RODO, Ustawy z dnia 10.05.2018r. o ochronie danych odpowiedzialność za ochronę danych osobowych spoczywa na Administratorze Danych Osobowych oraz na każdej osobie upoważnionej do dostępu do danych.

1. **Administrator Danych Osobowych zapewnia:**

- środki techniczne i organizacyjne niezbędne do zapewnienia bezpiecznego przetwarzania danych w pomieszczeniach do tego przeznaczonych – zabezpieczenie danych
- system i sprzęt informatyczny umożliwiający niezawodne i bezpieczne przetwarzanie danych
- dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie do przetwarzania danych osobowych
- spełnienie wskazanych w ustawie przesłanek legalizujących przetwarzanie danych osobowych;
- obowiązek informacyjny związany z pozyskaniem danych;
- obowiązek dochowania szczególnej staranności przy przetwarzaniu danych, w celu ochrony interesów osób, których dane dotyczą;
- obowiązek prowadzenia wymaganej dokumentacji min. rejestru czynności przetwarzania, rejestru incydentów, ewidencji osób upoważnionych, oceny skutków dla ochrony danych osobowych.
- przeszkolenie pracownika poprzez skierowanie nowo przyjętego pracownika do Inspektora ochrony danych

2. Pracownicy administratora (nauczyciele i pracownicy administracyjni i obsługi)

Personel administratora zobowiązany jest m.in.:

- zapoznać się oraz stosować postanowienia niniejszej Polityki ochrony danych osobowych
- zapoznać się z obowiązującymi przepisami w zakresie ochrony danych osobowych
- do ochrony przetwarzanych danych osobowych przed nieuprawnionym dostępem do tych danych, ich nieuzasadnioną modyfikacją lub zniszczeniem;
- korzystać z zasobów informatycznych oraz sprzętu w sposób zgodny z ich przeznaczeniem i w sposób bezpieczny, m.in. poprzez okresową zmianę haseł, zachowanie poufności loginów i haseł oraz niepozostawianie sprzętu bez nadzoru;
- niezwłocznego informowania przełożonych o zaobserwowanych nieprawidłowościach, które mogą mieć wpływ na bezpieczeństwo przetwarzanych danych osobowych;
- przechowywania dokumentacji zawierającej dane osobowe w przeznaczonych do tego miejscach, z ograniczonym dostępem osób trzecich, zwłaszcza dokumentacji zawierającej dane wrażliwe uczniów, rodziców/opiekunów prawnych;
- zachować w tajemnicy wszelkie dane osobowe, które pozyskał w trakcie wykonywania obowiązków służbowych.

Pracownik ponosi odpowiedzialność za należyte wykonywanie swoich obowiązków i jest on pouczony przez administratora o sankcjach wynikających z nieprawidłowości w tym zakresie, w tym o odpowiedzialności karnej.

§ 3 INSPEKTOR OCHRONY DANYCH

1. WYZNACZENIE INSPEKTORA OCHRONY DANYCH

Administrator wyznacza Inspektora Ochrony Danych. Wzory wyznaczenia stanowi **załącznik nr 1 do Polityki**. Wzór oświadczenia wyznaczonego Inspektora Ochrony Danych stanowi **załącznik nr 2 do Polityki**.

Administrator publikuje dane kontaktowe Inspektora Ochrony Danych i zawiadamia o nich organ nadzorczy. Administrator zapewnia, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

2. ZADANIA INSPEKTORA OCHRONY DANYCH

Administrator powierza Inspektorowi Ochrony Danych, realizację zadań określonych w art. 39 ust. 1 RODO.

Inspektor ochrony danych realizuje zadania w zakresie ochrony danych osobowych, takie jak, w szczególności:

a) informowanie Administratora oraz jego pracowników i współpracowników o spoczywających na nim (nich) obowiązkach wynikających z RODO oraz innych przepisów UE lub przepisów krajowych,
b) bieżące doradztwo wobec Administratora oraz jego pracowników i współpracowników w zakresie stosowania przepisów dotyczących ochrony danych osobowych,
c) monitorowanie przestrzegania przepisów dotyczących ochrony danych osobowych oraz niniejszej Polityki, w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu Administratora uczestniczącego w operacjach przetwarzania oraz prowadzenie powiązanych z powyższym audytów bezpieczeństwa,
d) udzielanie na żądanie zaleceń co do oceny skutków przetwarzania danych osobowych dla ich ochrony oraz monitorowania jej wykonania, zgodnie z art. 35.
e) współpraca z organem nadzorczym
f) 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.

Inspektor ochrony danych osobowych może pełnić swoje obowiązki z pomocą innych osób zatrudnionych lub niezatrudnionych przez Administratora.

Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

3. STATUS INSPEKTORA OCHRONY DANYCH

1. Administrator zapewnia, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
2. Administrator wspiera inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby i przedsięwzięcia niezbędne do utrzymania właściwego poziomu oraz aktualizacji jego wiedzy fachowej;
3. Administrator zapewnia, aby inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań.
4. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw im przysługujących;
5. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań;
6. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.

§ 4 POLITYKA RETENCJI DANYCH

1. Dane osobowe będą 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. Administrator jest uprawniony do przechowywania danych osobowych przez okres dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane, 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 RODO, 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.

2. Okres przechowywania danych osobowych został określony przez Administratora w treści prowadzonego Rejestru czynności przetwarzania na podstawie Instrukcji Kancelaryjnej i Jednolitego Wykazu Akt obowiązujących w placówce.

§ 5 PODSTAWOWE ZASADY ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH

1. Zakres obowiązywania

1. Ochrona danych osobowych przetwarzanych przez Administratora danych osobowych obowiązuje wszystkie osoby, które mają dostęp do danych osobowych podlegających przetwarzaniu, bez względu na zajmowane stanowisko oraz miejsce wykonywania, jak również charakter łączącej je umowy lub stosunku pracy z Administratorem danych osobowych.
2. Pracownicy oraz współpracownicy Administratora danych osobowych są zobligowani do stosowania niezbędnych środków zapobiegających ujawnieniu danych osobowych osobom nieupoważnionym, w tym w szczególności procedur wskazanych w niniejszej Polityce.
3. Zachowanie tajemnicy w zakresie danych osobowych obowiązuje zarówno podczas trwania stosunku pracy lub innej umowy łączącej Użytkownika z Administratorem danych osobowych, jak również po ustaniu stosunku pracy lub innej umowy.
4. Wszędzie, gdzie jest mowa o pracownikach, należy przez to rozumieć zarówno osoby zatrudnione w ramach stosunku pracy, jak również w oparciu o umowę cywilnoprawną (w tym umowę zlecenie oraz umowę o współpracy i o świadczenie usług).

Przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu przeznaczonych. Pomieszczenia, w których są przetwarzane przez ADO dane osobowe muszą być zamykane na klucz bądź powinny być wyposażone w innego rodzaju system umożliwiający blokadę wejścia do takiego pomieszczenia. Pomieszczenia, do których dostęp mają osoby nieupoważnione, osoby te mogą przebywać w tych pomieszczeniach jedynie w obecności osób upoważnionych oraz wyłącznie w czasie wymaganym na wykonanie niezbędnych czynności.

W szczególnych przypadkach możliwe jest przetwarzanie danych osobowych poza wyznaczonym obszarem przetwarzania jednak wymaga to decyzji ADO.

Zasady pracy zdalnej określają odrębne Procedury przyjęte przez Administratora - regulamin pracy zdalnej stanowi załącznik do regulaminu pracy.

Dostęp do pomieszczeń, w których są przetwarzane dane osobowe, lub przechowywane są kopie zapasowe, mogą mieć wyłącznie osoby, które posiadają do tego odpowiednie upoważnienie nadane przez ADO.

Przetwarzania danych osobowych może dokonywać wyłącznie osoba posiadająca upoważnienie do ich przetwarzania.

Wszystkie osoby przetwarzające dane osobowe z upoważnienia Administratora obowiązuje *zasada czystego biurka,* zabraniająca pozostawiania jakichkolwiek dokumentów z danymi osobowymi podczas nieobecności pracownika przy stanowisku pracy. Niedozwolone jest pozostawianie dokumentacji papierowej z danymi osobowymi na stanowisku pracy po jej zakończeniu, gdyż należy uniemożliwić zapoznanie się z danymi osobowymi osobom nieuprawnionym.

W przypadku opuszczenia stanowiska pracy osoba przetwarzająca dane osobowe powinna wylogować się z systemu lub zablokować dostęp do pulpitu stacji roboczej, z której korzysta przy przetwarzaniu danych osobowych. Ponadto w razie opuszczenia stanowiska pracy lub zakończenia pracy z systemem informatycznym należy zamykać pliki zawierające dane osobowe. Uniemożliwi to dostęp do danych osobowych osobie nieupoważnionej.

§ 6 ZARZĄDZANIE BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych

Na każdym etapie przetwarzania danych osobowych bez względu na zajmowane stanowisko, oraz miejsce wykonywania pracy należy brać pod uwagę, zasady z art. 5 czyli,

- **zgodność z prawem, rzetelność i przejrzystość** czyli przetwarzanie zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Zasada ta jest realizowana poprzez wypełnienie obowiązku informacyjnego.
- **ograniczenie celu** czyli zbieranie danych w konkretnych i wyraźnie uzasadnionych celach i nieprzetwarzanie dalej w sposób niezgodny z tymi celami
- **minimalizację danych**- stosowanie oraz ograniczenie do tego co niezbędne do celów, w których te dane są przetwarzane,
- **prawidłowość** czyli dane osobowe, które są przetwarzane są prawidłowe, a w razie potrzeby uaktualniane. Dane nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Każda osoba, które dane dotyczą ma prawo sprostowania danych zgodnie z art. 16 RODO.
- **ograniczenie przechowywania**- przechowywanie danych, które umożliwiają identyfikację osoby przez okres nie dłuższy niż niezbędne jest to 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, historycznych lub do celów statystycznych na mocy art. 89 ust. 1, 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.
- **integralność i poufność** - przetwarzanie danych w taki sposób, aby zapewnić bezpieczeństwo tym danym, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

§ 7 ZASADY UPOWAŻNIANIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Dostęp do danych osobowych oraz możliwość ich przetwarzania mają tylko osoby upoważnione przez Administratora Danych Osobowych. Administrator podejmuje działania w celu zapewnienia, by każda osoba fizyczna działająca z jego upoważnienia, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na jego polecenie, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

ADO nadaje upoważnienie do przetwarzania danych osobowych. Zmiana upoważnienia do przetwarzania danych osobowych następuje w przypadku zmiany zakresu przetwarzania danych osobowych np. w związku ze zmianą stanowiska pracy i jest niezwłocznie odnotowywane w ewidencji osób upoważnionych.

ADO prowadzi ewidencję osób upoważnionych do przetwarzania danych.

ADO powiadamia IOD o:

a) zatrudnieniu pracownika
b) ustaniu zatrudnienia pracownika
c) powrocie pracownika po okresie nieobecności co najmniej 30 dni np. po urlopie bezpłatnym, macierzyńskim itp.

1. Wzór upoważnienia do przetwarzania danych osobowych stanowi **załącznik nr 3 do Polityki**.
2. Wniosek o cofnięcie upoważnienia do przetwarzania danych osobowych- stanowi **załącznik nr 4 do Polityki.**
3. Wzór Oświadczenia o zachowaniu poufności stanowi **załącznik nr 5 do Polityki.**
4. Wzór oświadczenia o zachowaniu poufności dla pracowników, którzy nie są upoważnieni do przetwarzania danych osobowych stanowi załącznik **nr 6 do Polityki.**
5. Wzór ewidencji osób upoważnionych stanowi **załącznik nr 7 do Polityki**
6. Wykaz pomieszczeń, w których przetwarzane są dane osobowe **– stanowi załącznik nr 8 do Polityki**

§ 8 PROCEDURA NADAWANIA I ODBIERANIA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Osoba upoważniona do przetwarzania danych osobowych w Szkole Podstawowej im. KEN w Brzostku może przetwarzać dane osobowe wyłącznie w zakresie ustalonym przez Administratora Danych. Osobowych w indywidualnym upoważnieniu i tylko w celu określonym w upoważnieniu.
2. Zakres dostępu do danych osobowych przetwarzanych w formie papierowej i elektronicznej przypisany jest indywidualnie do każdego pracownika i został określony w imiennym upoważnieniu.

Procedura upoważniania do przetwarzania danych osobowych pracownika zatrudnionego w Szkole Podstawowej im. KEN e Brzostku przebiega w następujący sposób:

- Po przyjęciu do pracy Administrator Ochrony Danych kieruje pracownika do Inspektora Ochrony Danych w celu przeszkolenia z zakresu ochrony danych osobowych.
- Po zapoznaniu się pracownika z przepisami o ochronie danych osobowych Administrator Ochrony Danych przygotowuje dla pracownika upoważnienie oraz oświadczenie o zachowaniu poufności dot. przetwarzania danych osobowych, które zostaje przedstawione pracownikowi do podpisania. Upoważnienie oraz oświadczenie stanowią załącznik do Polityki Ochrony Danych.
- Podpisane upoważnienie i oświadczenie zostają dołączone do akt osobowych zgodnie z obowiązującymi przepisami – z Rozporządzeniem Ministra rodziny, pracy i polityki społecznej z dn. 10 grudnia 2018r. w sprawie dokumentacji pracowniczej [Dz.U.2018.2369 z późn. zm.] oraz 1 egz. dla pracownika.

Administrator Danych Osobowych wprowadza dane pracownika do Ewidencji osób upoważnionych.

Pracownik ma odebrane lub zaktualizowane upoważnienie do przetwarzania danych osobowych w sytuacji:

- Ustania stosunku pracy,
- Zmiany zakresu czynności lub stanowiska pracy, która powoduje konieczność zmiany w zakresie przetwarzania danych osobowych.

Aktualizacja upoważnienia wymaga **cofnięcia nieaktualnego** oraz nadania nowego upoważnienia do przetwarzania danych osobowych.

Procedura cofnięcia upoważnienia do przetwarzania danych osobowych przebiega w następujący sposób:

- Administrator Danych Osobowych przygotowuje dokument cofnięcia upoważnienia do przetwarzania danych osobowych.
- Podpisane cofnięcie upoważnienia zostaje dołączone do akt osobowych pracownika (1 egz.), oraz 1 egz. dla pracownika.

Rozwiązanie umowy o pracę powoduje utratę dostępu pracownika do przetwarzania danych osobowych bez konieczności przeprowadzania procedury odebrania upoważnienia do przetwarzania danych osobowych. Administrator Danych Osobowych odnotowuje ten fakt w Ewidencji upoważnień do przetwarzania danych Osobowych.

Administrator podejmuje działania w celu zapewnienia, by każda osoba fizyczna działająca z jego upoważnienia, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na jego polecenie, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

§ 9 DZIAŁANIA SZKOLENIOWE I UŚWIADAMIAJĄCE

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO. Szkolenia wszystkich nowozatrudnionych pracowników jest przeprowadzane w formie instruktażu przez IOD.
2. Szkolenia okresowe osób posiadających upoważnienie do przetwarzania danych osobowych przeprowadza się co trzy lata. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia szkolenia.

3. Administrator wprowadza zasadę realizacji działań upowszechniających poprzez informowanie pracowników o nowelizacjach dotyczących zasad ochrony danych osobowych.

§ 10 REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH / REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA DANYCH PODMIOTU PRZETWARZAJĄCEGO

1.Rejestr czynności przetwarzania Danych Osobowych stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności. Administrator danych osobowych lub inne osoby wskazane przez ADO zobowiązane **są do niezwłocznego informowania IOD** o wszelkich zmianach w zakresie danych osobowych oraz programów zastosowanych do przetwarzania danych osobowych.

2. Podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania danych.

Wzór rejestru czynności przetwarzania danych osobowych stanowi **załączniku nr 9** do Polityki.
Wzór rejestru kategorii czynności przetwarzania danych stanowi **załączniku nr 10** do Polityki.
Rejestry, o których mowa w ust. 1 i 2 prowadzi Inspektor Ochrony Danych w formie elektronicznej po zdobyciu informacji od Administratora danych osobowych. Rejestr w wersji elektronicznej i papierowej jest przechowywany przez Administratora ochrony danych.

§ 11 ZASADY UDOSTĘPNIANIA I POWIERZANIA PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator danych osobowych udostępnia dane osobowe przetwarzane we własnych zasobach tylko osobom lub podmiotom uprawnionym do ich otrzymania **na mocy przepisów prawa lub na podstawie zgody rodzica/opiekuna prawnego.**
2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe nie mające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.
3. W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia określa się przede wszystkim zobowiązania podmiotu przetwarzającego do:
   - przetwarzania danych wyłącznie na udokumentowane polecenie administratora;
   - zapewnienia, by osoby upoważnione do przetwarzania danych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
   - podejmowania środków zabezpieczenia danych wymaganych przez RODO i pomocy Administratorowi w wywiązywaniu się z tych obowiązków;
   - przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego, w tym między innymi za zgodą Administratora;
   - pomagania Administratorowi wywiązać się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania jej praw określonych w RODO;
   - usunięcia danych lub do zwrotu danych Administratorowi danych po zakończeniu przetwarzania, zgodnie z decyzją administratora;
   - udostępniania Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia jego obowiązków oraz do umożliwiania Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzania audytów.

§ 12 OCENA PODMIOTU PRZETWARZAJĄCEGO

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, będzie on korzystał wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
   W przypadku powierzenia danych osobowych innemu Administratorowi należy zawrzeć umowę powierzenia.
2. Wzór umowy powierzenia przetwarzania danych osobowych stanowi **załącznik nr 11 do Polityki**.
3. Rejestr umów powierzenia przetwarzania danych osobowych stanowi **załącznik nr 12 do Polityki.**

§ 13 PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH LUB ORGANIZACJI MIĘDZYNARODOWYCH

Nie dotyczy.

§ OGÓLNE ZASADY DOPEŁNIENIA OBOWIĄZKÓW INFORMATYCZNYCH

Każda osoba, której dane osobowe będą przetwarzane przez Administratora danych osobowych, ma prawo do bycia poinformowaną o przetwarzaniu danych osobowych. W związku z tym, wobec osób, których dane dotyczą, a których dane osobowe są przez Administratora danych osobowych przetwarzane, Administrator zobowiązany jest wypełniać obowiązek informacyjny wobec osób, których dane dotyczą, zgodnie z art. 13 RODO i art.14 RODO.

Obowiązek informacyjny Administrator spełnia przez przekazanie informacji poprzez stronę internetową, w biuletynie informacji publicznej, tablicy informacyjnej w placówce oraz na drukach na których są zbierane po raz pierwszy dane osobowe.

§ 11 PRZETWARZANIE NA PODSTAWIE ZGODY

1. W przypadku, gdy postawą przetwarzania jest zgoda osoby, której dane dotyczą, administrator, działając w celu wykazania, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych, stosuje:
a) oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych na podstawie art. 6 ust. 1 lit. a RODO, którego wzór stanowi **załącznik nr 13 do Polityki**;
b) oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych na podstawie art. 9 ust. 2 lit. a RODO, którego wzór stanowi **załącznik nr 14 do Polityki**.
2. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie i następuje z wykorzystaniem oświadczenia o wycofaniu zgody, które składa do Administratora lub bezpośrednio do Inspektora ochrony danych. Wycofanie zgody wzór stanowi **załącznik nr 15 do Polityki**.

§ 12 PROCEDURY REALIZACJI PRAW JEDNOSTKI.

1. Rodzic/ opiekun prawny osoby lub osoba której dane dotyczą, jest uprawniony do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dziecka dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do tych danych oraz uzyskania informacji określonych w art. 15 ROOD. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, jest informowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.

2. Administrator dostarcza osobie lub osobie której dziecka dane dotyczą, kopie danych osobowych podlegających przetwarzaniu, z zastrzeżeniem, iż za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator pobierze opłatę w wysokości wynikającej z kosztów administracyjnych, o czym informuje wnioskodawcę, przed dostarczeniem kopii danych.
3. Rodzic/ opiekun prawny dziecka lub osoba której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących danych osobowych dziecka, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, rodzic / opiekun prawny dziecka, którego dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
4. Rodzic / opiekun prawny dziecka lub osoba której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących danych osobowych jej dziecka, wyłącznie na zasadach określonych w art. 17 RODO.
5. **Obowiązek usunięcia danych nie będzie występował jeżeli Szkoła dysponuje podstawą prawną do ich przetwarzania.**
6. Rodzic / opiekun prawny dziecka lub osoba której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania jedynie w przypadkach, o których mowa w art. 18 RODO.
7. Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18 RODO, rodzica/ opiekuna prawnego każdego dziecka, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje rodzica / opiekuna prawnego dziecka, którego dane dotyczą, o tych odbiorcach, jeżeli rodzic/ opiekun prawny dziecka, którego dane dotyczą, tego zażąda.
8. Rodzic / opiekun prawny dziecka lub osoba której dane dotyczą, ma prawo otrzymać od administratora w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dziecka dotyczące, które dostarczyła administratorowi oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, wyłącznie na warunkach określonych w art. 20 RODO.
9. Rodzic / opiekun prawny dziecka lub osoba której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących danych osobowych jej dziecka opartego na art. 6 ust. 1 lit. e) lub f) RODO, w tym profilowania. Administrator nie będzie przetwarzać tych danych osobowych, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w art. 21 ust. 1 i 2 RODO oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji – sprzeciw wobec przetwarzania danych osobowych stanowi **załącznik nr 17 do Polityki**.
10. Wzór wniosku o uzyskanie kopii/dostęp/sprostowanie/usunięcie/przeniesienie/ograniczenie przetwarzania danych osobowych stanowi **załącznik nr 16 do Polityki**.
11. Rodzic / opiekun prawny dziecka lub osoba której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec dziecka skutki prawne lub w podobny sposób istotnie na nią wpływa, na zasadach określonych w art. 22 RODO.
12. Administrator udostępnia osobie, której dane dotyczą, żądane informacje i dane w formie pisemnej lub elektronicznej- wzór odpowiedzi na wniosek dotyczący realizacji praw jednostki **stanowi załącznik nr 18 do Polityki.**
13. Sposób realizowania praw jednostki:

a) uprawnienia wynikające z niniejszej procedury mogą być realizowane przez rodzica / opiekuna prawnego dziecka lub osoby, której dane dotyczą osobiście, procedurą w formie papierowej - pisemnej.
a) w przypadku zgłoszenia gdy żądanie zostanie zaadresowane na adres Szkoły Podstawowej im. KEN w Brzostku, żądanie przekazywane jest niezwłocznie przez administratora lub odpowiednio upoważniony personel do Inspektora Ochrony Danych.
b) kontakt z Inspektorem Ochrony Danych możliwy jest w biurze Centrum Usług Wspólnych w Brzostku, ul. M.N. Mysłowskiego 11, 39-230 Brzostek. Personel Szkoły informuje wnioskodawcę o możliwości osobistego kontaktu z Inspektorem, przekazując dodatkowo numer telefonu i adres poczty e-mail oraz wzór dokumentu zgłoszenia żądania.
c) w przypadku osobistego stawiennictwa w siedzibie Inspektora ochrony danych weryfikacja tożsamości rodzica/ opiekuna prawnego następuje poprzez porównanie danych wnioskodawcy z wniosku z wizerunkiem ze zdjęciem z dokumentu tożsamości.

14. Weryfikacja kompletności wniosku lub przesłanek wyłączających możliwość jego rozpoznania.
Po zweryfikowaniu tożsamości osoby ADO/Inspektor ochrony danych dokonuje weryfikacji przedmiotu wniosku pod kątem jego kompletności oraz czy wniosek nie jest nadmierny lub ewidentnie nieuzasadniony. W przypadku stwierdzenia braku wystarczających danych osobowych lub nadmierności wniosku lub jego ewidentnej niezasadności, odmawia rozpoznania wniosku, o czym informuje wnioskodawcę wraz z pouczeniem o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem oraz wyjaśnieniem przyczyn odmowy rozpoznania wniosku. W sytuacji gdy przyczyną odmowy rozpoznania wniosku jest brak odpowiednich danych lub konkretyzacji żądania, w wyjaśnieniu Administrator wraz z Inspektorem ochrony danych informują jakich danych zabrakło do rozpatrzenia wniosku.

Należy chronić dane osobowe przed wszelkim dostępem osób upoważnionych.

§ 13 ZABEZPIECZENIA INFORMATYCZNE

Przetwarzać dane osobowe w systemie informatycznym może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych.
W celu określenia zasad właściwego użytkowania i zarządzania systemem informatycznym służącym do przetwarzania danych osobowych ADO wdraża i stosuje Instrukcję Zarządzania Systemem Informatycznym co stanowi **załącznik nr 19 do Polityki**
Instrukcja Zarządzania Systemem Informatycznym reguluje kwestie:

a) Zasady bezpiecznego użytkowania sprzętu IT, programów
b) Procedur rozpoczęcia, zawieszenia i zakończenia pracy przeznaczonych dla użytkowników systemu
c) Polityka haseł
d) Zasady wynoszenia nośników z danymi poza placówkę
e) Zasady korzystania z Internetu
f) Zasady korzystania z poczty elektronicznej
g) Tworzenia kopii zapasowych zbiorów danych
h) Ochrona antywirusowa
i) Obowiązki zachowania poufności i ochrony danych osobowych
j) Użytkowanie komputerów przenośnych

§ 14 ZABEZPIECZENIA ORGANIZACYJNE

ADO zapewnia odpowiedni poziom bezpieczeństwa danych osobowych poprzez:

a) upoważnienia pracowników i oświadczenia o poufności do przetwarzania danych osobowych,

b) opracowanie niezbędnej dokumentacji – procedur i zasad składających się na Politykę ochrony danych osobowych
c) wdrożenie rozwiązań technicznych, zapewniających wymagany niniejszą Polityką poziom bezpieczeństwa przetwarzania informacji – inwestycję w infrastrukturę sieci i systemów informatycznych oraz fizyczne zabezpieczenie obszarów przetwarzania informacji chronionych.
d) Propagowanie zasad bezpieczeństwa wśród pracowników jednostki
e) Przeprowadzanie okresowych analiz ryzyka dla czynności przetwarzania danych osobowych w celu monitorowania w sposób ciągły zastosowanych zabezpieczeń pod względem prawidłowości ich funkcjonowania, aktualności oraz adekwatności w stosunku do zagrożeń
f) Dostosowanie środków ochrony danych do ustalonego poziomu ryzyka.
g) Wdrożenie i stosowanie Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w celu zapewnienia bezpieczeństwa danych osobowych przed zagrożeniami np. nieautoryzowaną modyfikacją, utratą, szkodzeniem, udostępnieniem osobom nieupoważnionym
h) Szkolenia z zakresu ochrony danych i obowiązujących w tym zakresie przepisów
i) Opracowanie, prowadzenie i utrzymanie Rejestr Czynności Przetwarzania Danych Osobowych
j) Każda osoba mająca dostęp do danych przetwarzała je wyłącznie na polecenie ADO
k) Bez względu na zajmowane stanowisko, charakter stosunku pracy, zasady określone w niniejszej Polityce oraz w dokumentach powiązanych muszą być znane i stosowane przez pracowników jednostki
l) W przypadku powierzania przetwarzanych danych osobowych konieczne jest zawarcie umowy powierzenia
m) ADO wydaje upoważnienia do przetwarzania danych osobowych
n) Przed przyznaniem dostępu do danych osobowych pracownik musi zostać zapoznany przez IOD z przepisami stosowania polityki ochrony danych osobowych, obowiązującymi uregulowaniami wewnętrznymi w w/w zakresie. Na potwierdzenie czego składa oświadczenie o poufności osoby upoważnionej
o) niepozostawianie pomieszczenia w czasie pracy bez nadzoru,
Pomieszczenia, w których są przetwarzane przez ADO dane osobowe muszą być zamykane na klucz bądź powinny być wyposażone w innego rodzaju system umożliwiający blokadę wejścia do tego pomieszczenia. Osoby nieupoważnione mogą przebywać jedynie w obecności osób upoważnionych.
p) Miejsca np. szafy, szafki przeznaczone do przechowywania danych osobowych muszą być zamykane na klucz lub powinny być wyposażone w innego rodzaju system umożliwiający blokadę otwarcia takich miejsc. Klucze do tych miejsc posiadają wyłącznie pracownicy upoważnieni.
q) Miejsca z danymi osobowymi są otwarte tylko na czas potrzebny na dostęp do tych danych, a następnie zostają zamknięte. Dokumenty zawierające dane osobowe należy przenieść do odpowiednio zabezpieczonego miejsca. **Wprowadzono** politykę kluczy która stanowi **załącznik nr 21 do Polityki,**
r) Wprowadzono i zobowiązano pracowników do stosowania polityki czystego biurka i czystego ekranu – **załącznik nr 20 do Polityki.**
s) Wydruki robocze, które zawierają dane osobowe błędne lub zdezaktualizowane muszą być niezwłocznie trwale zniszczone przy użyciu niszczarki do papieru, zapewniający skuteczne ich usunięcie lub pseudonimizację.
t) Zasady dostępu do budynków określają odrębne polecenia służbowe Administratora.

§ 15 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**”. Polega ona na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach

przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach
3. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych lub w lesie.

§ 16 MONITOROWANIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych.
2. Zgodnie z art. 28 RODO Procesor Administrator może zweryfikować przestrzeganie obowiązujących zasad ochrony danych u Procesora.

§ 17 METODYKA ZARZĄDZANIA RYZYKIEM

1. Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
2. Wszędzie gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.
3. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

§ 18 UWZGLĘDNIANIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA DANYCH- PRIVACY BY DEFAULT/DESIGN.

Zgodnie z art. 25 RODO Administrator wdraża odpowiednie środki techniczne i organizacyjne w celu skutecznej realizacji zasad ochrony danych takich jak polityka bezpieczeństwa, i procedury bezpieczeństwa w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których prawa dotyczą.

§ 19 PROCEDURA POSTĘPOWANIA W RAZIE NARUSZENIA ORAZ PROCEDURA POWIADOMIENIA O NARUSZENIU DANYCH

Odpowiedzialni za wykonanie procedury

1. Inspektor ochrony danych w zakresie:
   A. Oceny czy zgłoszenie stanowi naruszenie ochrony danych osobowych
      1) Jeżeli TAK – czy może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych i w związku z tym zgłoszenie organowi nadzorczemu
      2) Jeżeli NIE – kończy postępowanie i informuje zgłaszającego
   B. Dokumentowania spraw z zakresu naruszeń
2. Administrator ochrony danych
   A. Ewentualne zgładzenie naruszenia zgłasza do Urzędu Ochrony Danych Osobowych
   B. Ewentualne informowanie osób, których dane dotyczą o wystąpieniu naruszenia
3. Administrator systemu informatycznego (ASI) – w sytuacji, gdy naruszenie dotyczy systemów informatycznych, współdziała z IOD
4. Pracownicy – w zakresie zgłoszenia podejrzenia naruszenia lub naruszenia danych osobowych

Zgłaszanie incydentów związanych z bezpieczeństwem informacji

1. Każdy pracownik, stażysta, wolontariusz, praktykant oraz osoba realizująca zadania na podstawie umowy cywilnoprawnej, którzy stwierdzili lub podejrzewają wystąpienie zdarzenia, które stanowi naruszenie ochrony danych osobowych, ma obowiązek zgłoszenia tego faktu bezpośredniemu przełożonemu oraz lub IOD. Zgłoszenie w formie ustnej musi być potwierdzone w formie elektronicznej lub na piśmie. Osoba zgłaszająca odpowiada za wyczerpujący opis incydentu odpowiednio do posiadanej wiedzy i umiejętności.

2. Zgłoszenie zdarzenia mogącego być naruszeniem ochrony danych osobowych musi zawierać:
   1) Imię i nazwisko osoby zgłaszającej
   2) Miejsce i datę wystąpienia incydentu
   3) opisanie symptomów naruszenia ochrony danych osobowych;
   4) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
   5) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia;
   6) określenie znanych danej osobie sposobów zabezpieczenia oraz wszelkich kroków podjętych po ujawnieniu zdarzeń.

Brak umiejętności poprawnego rozpoznania incydentu przez osobę zgłaszającą nie może być przyczyną zaniechania zgłoszenia.

3. Stwierdzenie naruszenia następuje w momencie, kiedy IOD ma wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, prowadzące do naruszenia bezpieczeństwa danych osobowych.

4. Jeżeli naruszenie ochrony danych osobowych dotyczy systemu informatycznego, ASI w porozumieniu z IOD podejmuje niezbędne działania zabezpieczające niezwłocznie po otrzymaniu informacji, o której mowa w ust. 3. Szczegółowe zasady w tym zakresie opisuje Polityka bezpieczeństwa informacji.

5. Jeżeli naruszenie ochrony danych nie dotyczy systemu informatycznego i ma związek z naruszeniem zabezpieczeń fizycznych, odpowiednie czynności zabezpieczające podejmuje IOD, tj.:
   1) nakazuje przerwanie pracy, zwłaszcza w zakresie przetwarzania danych osobowych, do czasu powiadomienia o zaistniałej sytuacji Administratora danych osobowych
   2) działa w celu wyjaśnienia okoliczności zdarzenia;
   3) przedstawia zalecenia w celu umożliwienia dalszego bezpiecznego przetwarzania danych.

6. Odmowa udzielenia wyjaśnień lub współpracy z IOD traktowana będzie jako naruszenie obowiązków pracowniczych.

7. Raport o naruszeniu danych osobowych opracowuje IOD – wzór raportu stanowi **załącznik nr 23 do Polityki.**

Działania w związku ze zgłoszonymi incydentami związanymi z naruszeniem danych osobowych

1. Zgłoszenie incydentu rejestrowane jest przez ADO w rejestrze incydentów związanych z naruszeniem ochrony danych osobowych.
   Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcia niezabezpieczonych materiałów zawierających dane osobowe itp.).
   Działania związane z obsługą zgłoszenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy zgłoszenie zostało zakwalifikowane jako incydent naruszenia bezpieczeństwa przetwarzania danych osobowych, dokonywana jest ocena jego istotności.
2. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
   1) Charakter naruszenia ochrony danych osobowych
   2) Kategorię i przybliżoną liczbę osób których dane dotyczą
   3) Możliwe konsekwencje naruszenia ochrony danych osobowych

4) Wpływ incydentu na ciągłość działania jednostki
5) Koszty usunięcia skutków incydentu
6) Szacowany czas naprawy skutków wywołanych incydentem

3. Zakwalifikowane zgłoszenie incydentu jako „fałszywy alarm" kończy postępowanie, o czym IOD informuje zgłaszającego.
4. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji, IOD podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu. W przypadku incydentu dotyczącego systemów informatycznych działania te są prowadzone w porozumieniu z ASI.

Działania w sytuacji stwierdzenia naruszenia ochrony danych osobowych

1. W przypadku naruszenia ochrony danych osobowych mają zastosowanie przepisy art. 33-34 rozporządzenia Parlamentu Europejskiego i Rady (UE)2016/679 z dn. 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych - RODO (Dz.Urz. UE L 119 z 5 kwietnia 2016r.))
2. W przypadku zakwalifikowania zdarzenia jako naruszenie ochrony danych osobowych ADO bez zbędnej zwłoki dokonuje zgłoszenia naruszenia do organu nadzorczego. Zgłoszenia w miarę możliwości dokonuje nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
3. Zgłoszenie dokonywane jest w formie przyjętej przez organ nadzorczy. Treść zgłoszenia zawiera elementy wskazane w art. 33 ust. 3 RODO.
4. **Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.** Zawiadomienie ma formę pisemną. Zawiadomienie nie jest wymagane w sytuacjach wskazanych w art. 34 ust. 3 RODO.
5. Jeżeli zawiadomienie osób, których dane dotyczą wymagałoby niewspółmiernie dużego wysiłku, ADO przygotowuje publiczny komunikat lub wybiera inny stosowny środek, za pomocą którego zawiadomienie zostanie tym sposobem przekazane.
6. ADO wraz z IOD podejmują również działania zabezpieczające i naprawcze zmierzające do zniwelowania skutków powstałych w wyniku incydentu, jak również działania zaradcze dla uniknięcia wystąpienia podobnych incydentów w przyszłości.
7. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze oraz prowadzi rejestr naruszeń.
8. Wszelkie naruszenia dokumentowane są przez Administratora Danych Osobowych zgodnie z art. 33 ust. 5 ogólnego rozporządzenia o ochronie danych.
9. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi, zgodnie z postanowieniami umowy o powierzenie przetwarzania danych osobowych, zawartej z podmiotem przetwarzającym.
10. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa przetwarzania danych osobowych Administrator podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie w zależności od wagi incydentu mogą być zawiadomione organy ścigania.

Odpowiednie wzory dokumentów, do wypełnienia obowiązków z art. 33 załączone są jako załączniki do Polityki pod nazwą:

- Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych stanowi **załącznik nr 24 do Polityki.**
- Raport z naruszeń danych osobowych (wewnętrzny) **załącznik nr 23 do Polityki.**
- Rejestr incydentów i działań korygujących dot. ochrony danych osobowych stanowi **załącznik nr 25 do Polityki.**

§ 20 OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

1. Możliwe zagrożenia dotyczące naruszenia ochrony danych osobowych

Podział zagrożeń:

a) **zagrożenia losowe zewnętrzne** – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu informatycznego, a zatem ciągłość systemu informatycznego zostaje zakłócona, ale w przypadku takich zagrożeń nie dochodzi do naruszenia poufności danych, np. klęski żywiołowe, przerwy w zasilaniu itp.,

b) **zagrożenia losowe wewnętrzne** – ich występowanie może prowadzić do zniszczenia danych, zakłócenia ciągłości pracy systemu informatycznego oraz do naruszenia poufności danych, np. niezamierzone pomyłki operatorów, Administratora, Podmiotu przetwarzającego, awarie sprzętowe, błędy oprogramowania, pogorszenie jakości sprzętu i oprogramowania,

c) **zagrożenia zamierzone** – świadome i celowe działania powodujące naruszenie poufności danych, zazwyczaj nieskutkujące uszkodzeniem infrastruktury technicznej i zakłóceniem ciągłości pracy; zagrożenia te można podzielić na:
   - nieuprawniony dostęp do systemu informatycznego z zewnątrz (włamanie do wskazanych systemów),
   - nieuprawniony dostęp do systemu informatycznego z jego wnętrza,
   - nieuprawnione przekazanie danych,
   - bezpośrednie zagrożenie materialnych składników systemu informatycznego (np. kradzież sprzętu).

Naruszenie lub podejrzenie naruszenia systemu informatycznego, w którym przetwarzane są dane osobowe, następuje w sytuacji:

a) losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych na zasoby systemu, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne itp.,
b) niewłaściwych parametrów środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych,
c) awarii sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych,
d) pojawienia się odpowiedniego komunikatu alarmowego,
e) podejrzenia nieuprawnionej modyfikacji danych w systemie lub innego odstępstwa od stanu oczekiwanego,
f) naruszenia lub próby naruszenia integralności systemu lub bazy w tych systemach,
g) pracy w systemie wykazującej odstępstwa uzasadniające podejrzenie przełamania lub zaniechania ochrony danych osobowych, jak np. praca osoby, która nie jest formalnie dopuszczona do obsługi systemu,
h) ujawnienia nieautoryzowanych kont dostępu do systemu,
i) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce itp.).

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych, jak np.:

a) niezabezpieczone pomieszczenia,

b) pozostawianie danych w nieodpowiednich miejscach (m.in. w koszach na śmieci czy w miejscach publicznie dostępnych),
c) pozostawienie niezabezpieczonych dokumentów zawierających dane osobowe na stanowisku pracy w razie jego opuszczenia przez osobę przetwarzającą dane w imieniu Administratora.

Przyczyny incydentów mogą dotyczyć:

- Niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową
- Działania szkodliwego oprogramowania
- Próby omijania systemów zabezpieczeń
- nieautoryzowanego dostępu do systemów, aplikacji i dokumentów
- zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji
- zniszczenia lub kradzieży nośników danych
- próby wyłudzeń informacji
- ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji
- nieprawidłowości w zakresie zabezpieczenia przechowywanych danych osobowych
- naruszenia zasad obowiązujących w jednostce np. pozostawienie włączonego komputera i /lub nie wylogowanie się po zakończeniu pracy lub podczas przerwy w pracy, pozostawienie niezabezpieczonych dokumentów zawierających dane osobowe itp.

.....

Administrator danych osobowych

Ustala się wykaz załączników do Polityki Bezpieczeństwa:

1. *Załącznik nr 1 do Polityki – wzór wyznaczenie IOD*
2. *Załącznik nr 2 do Polityki –wzór Oświadczenie IOD*
3. *Załącznik nr 3 do Polityki –wzór Upoważnienie do przetwarzania danych osobowych*
4. *Załącznik nr 4 do Polityki –wzór cofnięcie upoważnienia*
5. *Załącznik nr 5 do Polityki – wzór Oświadczenie o zachowaniu poufności osoby upoważnionej*
6. *Załącznik nr 6 do Polityki – wzór Oświadczenie o zachowaniu poufności dla osoby nie posiadającej obsługi*
7. *Załącznik nr 7 do Polityki – wzór Ewidencji osób upoważnionych do przetwarzania danych*
8. *Załącznik nr 8 do Polityki – wzór wykaz pomieszczeń, w których przetwarzane są dane osobowe*
9. *Załącznik nr 9 do Polityki – wzór Rejestru czynności przetwarzania*
10. *Załącznik nr 10 do Polityki – wzór Rejestru Kategorii czynności przetwarzania*
11. *Załącznik nr 11 do Polityki – wzór Umowa powierzenia*
12. *Załącznik nr 12 do Polityki – wzór Rejestr umów powierzenia*
13. *Załącznik nr 13 do Polityki – wzór Oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych zwykłych*
14. *Załącznik nr 14. do Polityki – wzór Oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych wrażliwych*
15. *Załącznik nr 15 do Polityki – wzór wniosek o cofnięcie zgody na przetwarzanie danych osobowych*
16. *Załącznik nr 16 do Polityki – wzór wniosek realizacja praw jednostki*
17. *Załącznik nr 17 do Polityki – wzór Sprzeciw wobec przetwarzania danych osobowych*
18. *Załącznik nr 18 do Polityki – wzór odpowiedź na wniosek - realizacja praw jednostki*
19. *Załącznik nr 19 do Polityki – wzór Instrukcja Zarządzania Systemem Informatycznym*
20. *Załącznik nr 20 do Polityki – wzór Polityka czystego biurka i czystego ekranu*
21. *Załącznik nr 21 do Polityki – wzór Polityka Kluczy*
22. *Załącznik nr 22 do Polityki – wzór Metodyka zarządzania ryzykiem w Szkole Podstawowej im. KEN w Brzostku*
23. *Załącznik nr 23 do Polityki – wzór Raport z naruszenia danych osobowych*
24. *Załącznik nr 24 do Polityki – wzór Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych*
25. *Załącznik nr 25 do Polityki – wzór Rejestr naruszeń w Szkole Podstawowej im. KEN w Brzostku*