POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Zespół Szkół Nr 2 im. Marii Skłodowskiej - Curie w Kwidzynie

Data obowiązywania:	25 maja 2018 r.
Podstawa prawna:	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); Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

1. Wykaz podstawowych definicji

Ilekroć w niniejszej Polityce Bezpieczeństwa Danych Osobowych mowa o:

Administratorze Danych Osobowych – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

Administratorze Systemu Informatycznego – rozumie się przez to pracownika Administratora Danych Osobowych lub inne osoby odpowiedzialne za funkcjonowanie oraz za przestrzeganie zasad i wymogów bezpieczeństwa systemów informatycznych;

Systemie informatycznym – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

Inspektorze Ochrony Danych – rozumie się przez to osobę odpowiedzialną za bieżący nadzór stosowania przepisów dot. ochrony danych osobowych;

Osobie upoważnionej – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych.

Danych osobowych – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Przetwarzaniu danych osobowych – rozumie się przez to 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;

Zbiorze danych osobowych – rozumie się przez każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

Podmiocie przetwarzającym – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych Osobowych;

Odbiorcy danych - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postepowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

Bezpieczeństwie danych osobowych – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania danych osobowych, by w każdych okolicznościach dostęp do nich był zgodny z założeniami i zapewniał ich poufność, integralność oraz dostępność;

Poufności danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;

Integralności danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

Dostępności danych – rozumie się przez to właściwość zapewniającą, że dane są osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie, przez uprawnioną osobę lub podmiot;

Zgodzie osoby, której dane dotyczą – rozumie się przez to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli przez osobę, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwalające na przetwarzanie dotyczących jej danych osobowych;

Państwie trzecim – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;

Naruszeniu ochrony danych osobowych - rozumie się przez to naruszenie bezpieczeństwa danych osobowych prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

2. Wprowadzenie

1. Polityka Bezpieczeństwa Danych Osobowych określa zestaw praw, zasad i zaleceń regulujących proces zarządzania informacją w kontekście bezpieczeństwa informacji i ochrony danych osobowych.
2. Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń techniczno - organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.
3. Niniejszy dokument jest zgodny z Rozporządzeniem 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 oraz Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych.
4. W Polityce Bezpieczeństwa Danych Osobowych stosuje się również przepisy ustaw i aktów wykonawczych, które odnoszą się do bezpieczeństwa informacji i ochrony danych osobowych.

3. Cele Polityki Bezpieczeństwa Danych Osobowych

Celem Polityki Bezpieczeństwa Danych Osobowych jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych sposobu zarządzania informacją w kontekście bezpieczeństwa informacji i ochrony danych osobowych.

4. Zakres stosowania Polityki Bezpieczeństwa Danych Osobowych

Zakres stosowania ochrony danych osobowych określone przez Politykę Bezpieczeństwa Danych Osobowych oraz inne z nią związane dokumenty mają zastosowanie do:

a. wszystkich istniejących, wdrażanych w przyszłości systemów informatycznych oraz dokumentów w formie papierowej i elektronicznej, w których przetwarzane są dane osobowe podlegające ochronie,
b. wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
c. wszystkich pracowników, współpracowników i innych osób mających dostęp do informacji podlegających ochronie.

5. Inspektor Ochrony Danych

2. Inspektor Ochrony Danych monitoruje przestrzeganie zasad bezpieczeństwa oraz prowadzi kontrolę przetwarzania danych osobowych.
3. Inspektor Ochrony Danych wykonuje w szczególności następujące zadania:
   a. zapewnienie przestrzegania przepisów dotyczących ochrony danych osobowych,
   b. opiniowanie, pod względem zgodności z Polityką Bezpieczeństwa Danych Osobowych oraz z przepisami prawa, umów, procedur i innych wytworzonych dokumentów dotyczących bezpieczeństwa i przetwarzania danych osobowych;
   c. podejmowanie lub wnioskowanie o podjęcie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych oraz prowadzenie adekwatnej dokumentacji w tym zakresie.
4. Inspektor Ochrony Danych może wykonywać swoje obowiązki poprzez wyznaczonych zastępców.
5. Administrator Danych Osobowych upoważnia Inspektora Ochrony Danych do przetwarzania danych osobowych we wszystkich zbiorach Administratora Danych Osobowych oraz poza nimi w zakresie niezbędnym dla należytego wykonywania funkcji Inspektora Ochrony Danych.

6. Podstawowe zasady ochrony danych osobowych

1. Wszystkie dane osobowe w Zespole Szkół Nr 2 im. Marii Skłodowskiej - Curie w Kwidzynie należy przetwarzać zgodnie z obowiązującymi przepisami prawa.
2. W stosunku do osób, których dane osobowe są przetwarzane należy spełnić obowiązek informacyjny.
3. Realizacja obowiązku informacyjnego może być w formie pisemnej, dźwiękowej, poprzez warstwowe przekazywanie informacji lub łączenie różnych form informowania.
4. Zebrane dane osobowe należy przetwarzać dla oznaczonych i zgodnych z prawem celów i nie poddawać dalszemu przetwarzaniu niezgodnemu z tymi celami.
5. Należy zadbać, aby przetwarzanie danych osobowych odbywało się zgodnie z zasadami dotyczącej merytorycznej poprawności oraz adekwatnie do celów w jakich zostały zebrane.

6. Dane osobowe można przetwarzać nie dłużej niż jest to niezbędne do osiągnięcia celu ich przetwarzania.
7. Należy zapewnić poufność, integralność oraz rozliczalność przetwarzanych danych osobowych.
8. Przetwarzane dane osobowe nie mogą być udostępniane bez zgody osób, których dane dotyczą, chyba że udostępnia się te dane osobom, których dane dotyczą, osobom upoważnionym do przetwarzania danych osobowych, podmiotom którym przekazano dane na podstawie umowy powierzenia oraz organom państwowym lub organom samorządu terytorialnego w związku z prowadzonym postępowaniem.
9. Przetwarzanie danych osobowych może odbywać się zarówno w systemach informatycznych, jak i w formie tradycyjnej (papierowej): kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.
10. Wszystkim osobom, których dane są przetwarzane przysługuje prawo do ochrony danych ich dotyczących, do kontroli przetwarzania tych danych oraz do ich uaktualniania, usunięcia, jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.

7. Upoważnienie do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych w formie papierowej i elektronicznej mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania danych osobowych.
2. Każdy użytkownik przed dopuszczeniem do pracy z danymi osobowymi winien być przeszkolony w zakresie ochrony danych osobowych.
3. Za przeprowadzenie szkolenia odpowiada Administrator Danych Osobowych i Inspektor Ochrony Danych.
4. Administrator Danych Osobowych prowadzi ewidencje:
   - Pracowników, współpracowników i innych osób upoważnionych do przetwarzania danych osobowych,
   - podmiotów przetwarzających,
   - firm świadczących usługi, w ramach których przetwarzane są dane osobowe.
5. Upoważnienia do przetwarzania danych osobowych sporządzane są w dwóch egzemplarzach.

6. Upoważnienia do przetwarzania danych osobowych nadawane są:
    a. pracownikom i współpracownikom Zespołu Szkół Nr 2 im. Marii Skłodowskiej - Curie w Kwidzynie;
    b. osobom odbywającym wolontariat, praktykę lub staż w Zespole Szkół Nr 2 im. Marii Skłodowskiej - Curie w Kwidzynie ;
    c. pracownikom podmiotów przetwarzających.
7. Firmy świadczące usługi na rzecz Zespołu Szkół Nr 2 im. Marii Skłodowskiej - Curie w Kwidzynie, w przypadku przetwarzania danych osobowych, zobowiązane są do:
    a. przestrzegania zasad ochrony danych osobowych, które powinny być zawarte w umowach lub oświadczeniach o zastosowanej polityce prywatności;
    b. zaznajomienia pracowników firmy z regułami postępowania z danymi osobowymi oraz informacjami stanowiącymi tajemnicę Zespołu Szkół Nr 2 im. Marii Skłodowskiej - Curie w Kwidzynie.
8. Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy:
    a. zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych;
    b. stosowanie się do zaleceń Inspektora Ochrony Danych;
    c. przetwarzania danych osobowych wyłącznie w zakresie ustalonym przez Administratora Danych Osobowych w pisemnym upoważnieniu;
    d. przetwarzanie danych osobowych tylko w celu wykonywania nałożonych obowiązków służbowych;
    e. niezwłoczne informowanie Inspektora Ochrony Danych o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych;
    f. ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem, usunięciem;
    g. korzystanie z systemów informatycznych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemów informatycznych;
    h. bezterminowe zachowanie w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
    i. zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których dane dotyczą.

8. Powierzenie przetwarzania danych osobowych

1. Administrator Danych Osobowych może zlecić innemu podmiotowi przetwarzanie danych osobowych w celu realizacji określonego zadania.
2. W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora danych osobowych oraz podmiotu przetwarzającego.

9. Udostępnianie danych osobowych

1. Dane osobowe udostępnia się:
   a) na pisemny wniosek;
   b) drogą elektroniczną, uwierzytelnioną podpisem kwalifikowanym lub ePUAP organu.
2. Wnioskodawca wskazuje na jakiej podstawie żąda udostępnienia danych, zaś administrator powinien zweryfikować tę podstawę – co do jej aktualności i trafności.
3. Wniosek o udostepnienie danych, który wpłynął do Zespołu Szkół Nr 2 im. Marii Skłodowskiej - Curie w Kwidzynie rozpatruje Właściciel zbioru.
4. Wniosek o udostepnienie danych osobowych, którego sposób rozpatrzenia budzi uzasadnione wątpliwości, może zostać przesłany, wraz z informacjami niezbędnymi dla jego rozpatrzenia, do Inspektora Ochrony Danych w celu zajęcia stanowiska w sprawie.

   Do wniosku dołącza się projekt odpowiedzi wraz z uzasadnieniem.
5. Informacje, zawierające dane osobowe są udostępniane uprawnionym podmiotom:
   a) w formie wydruku listem poleconym lub za potwierdzeniem osobistego odbioru;
   b) w drodze teletransmisji danych, w sposób gwarantujący poufność przesyłanych danych;
   c) na elektronicznych nośnikach informacji, za potwierdzeniem odbioru.
6. Ewidencja wniosków udostepnienia danych prowadzona jest przez Właścicieli zbiorów w wersji elektronicznej lub papierowej.

10. Ewidencja dokumentów

1. Ewidencja dokumentów regulujących ochronę danych osobowych w Zespole Szkół Nr 2 im. Marii Skłodowskiej - Curie w Kwidzynie stanowi załącznik do Polityki Bezpieczeństwa Danych Osobowych.
2. Dokumenty regulujące ochronę danych osobowych w Zespole Szkół Nr 2 im. Marii Skłodowskiej - Curie w Kwidzynie są aktualizowane decyzją Administratora Danych Osobowych.

11. Przekazywanie danych osobowych poza Polskę

1. Administrator Danych Osobowych może przekazywać dane osobowe do:
   - państw Europejskiego Obszaru Gospodarczego (EOG);
   - pozostałych państw (państwa trzecie);
   - organizacji międzynarodowych.
2. Przekazywanie danych osobowych w ramach EOG traktuje się tak, jakby były przetwarzane na terenie Polski.
3. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej następuje zgodnie z art. 44 – 49 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.

12. Naruszenie danych osobowych - odpowiedzialność

1. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w procedurach Polityki Bezpieczeństwa Danych Osobowych, a w szczególności nie powiadomiła Administratora Danych Osobowych lub Inspektora Ochrony Danych, wszczyna się postępowanie dyscyplinarne lub porządkowe.
2. Kara dyscyplinarna wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującymi przepisami lub możliwości wniesienia wobec niej sprawy z powództwa cywilnego.