Polityka Ochrony Danych Osobowych w Gimnazjum Gminnym w Siemiatyczach

I. Wykaz zabezpieczeń

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora danych w Gimnazjum Gminnym w Siemiatyczach w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

II. Wykaz zabezpieczeń

1. Dane osobowe wymagające ochrony administrator danych opracował w postaci papierowej, stanowiącej załącznik nr 1 do Polityki Ochrony Danych.

2. Wykaz obejmuje zbiory ze stwierdzonym potencjalnym ryzykiem naruszenia praw lub wolności osób fizycznych.

3. Każdy ze zbiorów jest opisany w sposób umożliwiający przeprowadzenie analizy ryzyka.

4. W szkole została opracowana Polityka Zarządzaniem ryzykiem w przetwarzaniu Danych Osobowych, określająca zasady szacowania skali ryzyka i prawdopodobieństwa jego wystąpienia.

5. Opis zbiorów obejmuje takie informacje, jak:
    1) nazwę zbioru;
    2) opis celów przetwarzania;
    3) charakter, zakres, kontekst, dokumentowane dane osobowe;
    4) odbiorcy;
    5) funkcjonalny opis operacji przetwarzania;
    6) aktywa służące do przetwarzania danych osobowych (Informacje, Programy, systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing);
    7) informacja o konieczności wpisu do rejestru czynności przetwarzania;
    8) informacja o konieczności przeprowadzenia oceny skutków dla zbioru.

6. Administrator, w uzgodnieniu z Inspektorem Ochrony Danych, opracował karty zawierające analizę ryzyka dla poszczególnych operacji przetwarzania danych w zakresie aktywów biorących udział w przetwarzaniu danych.

III. Zapewnienie o przetwarzania danych osobowych zgodnie z prawem.

1. Administrator zapewnia, że:

   1) dane osobowe są przetwarzane legalnie na podstawie art. 6 i 9 RODO;

   2) zakres danych osobowych jest adekwatny do celów przetwarzania, z zachowaniem zasady minimalizacji danych;

   3) Administrator przechowuje dane osobowe przez konkretnie określony czas, z uwzględnieniem zasad określonych w Jednolitym Rzeczowym Wykazie Akt, zatwierdzonym przez Archiwum Państwowe w Białymstoku ;

   4) wobec osób, których dane są przetwarzane wykonano obowiązek informacyjny (art. 12, 13, 14 RODO) wraz ze wskazaniem im: prawa dostępu do danych osobowych, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, „bycia zapomnianym";

   5) osoby, których dane osobowe są przetwarzane zostały poinformowane o funkcji IOD i przekazano dane kontaktowe;

   6) zapewniono ochronę danych osobowych w przypadku powierzenia danych w postaci umów powierzenia z podmiotami przetwarzającymi (art. 28 RODO).

2. Potwierdzenie przetwarzania danych osobowych zgodnie z prawem znajduje się z załączniku nr 1 – Wykaz Zbiorów Danych Osobowych.

3. Wzory klauzul informacyjnych znajdują się z załączniku nr 2– Klauzule Informacyjne.

III. Upoważnienia

1. Administrator odpowiada za nadawanie/anulowanie upoważnień do przetwarzania danych w zbiorach papierowych i systemach informatycznych.

2. Każda osoba upoważniona może przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.

3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych.

4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia.

5. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych załącznik nr 3 - Ewidencja osób upoważnionych.

IV. Procedura analizy ryzyka i ocena skutków.

1. Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.

2. Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru danych osobowych lub grupy zbiorów charakteryzujących się podobieństwem celów i sposobów przetwarzania/ odrębnie dla każdego zbioru.

3. W przypadku konieczności przeprowadzenia oceny skutków (art. 35) wykonano następujących czynności:

   I. dokonano opisu planowanych operacji przetwarzania i celów przetwarzania – załącznik nr 1 – Wykaz zbiorów danych osobowych;

   II. określono zagrożenia we wszystkich aktywach biorących udział w procesie przetwarzania;

   III. dokonano oceny ryzyka, zgodnie z zasadami wskazanymi w Polityce Zarządzania Ryzykiem;

   IV. sporządzono mapę ryzyka ze wskazaniem istotności ryzyka;

   V. zaplanowano środki techniczne, organizacyjne i informatyczne dla ryzyk przekraczających istotność powyżej 4.

V. Instrukcja postepowania z incydentami

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego lubInspektora Ochrony Danych.

2. Do typowych podatności bezpieczeństwa danych osobowych należą:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
   3) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
   2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych);
   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).

4. W przypadku stwierdzenia wystąpienia incydentu, Administrator lub IOD prowadzi postępowanie wyjaśniające w toku, którego:
   1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
   2) proponuje ewentualne działania dyscyplinarne;
   3) proponuje działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu;
   4) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, wtym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze –załącznik nr 4 Formularz rejestracji incydentu.

6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.

7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

VI. Regulamin Ochrony Danych

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

VII. Procedura przywracania dostępności danych osobowych

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Administrator opracował Procedury Przywracania Danych – załącznik nr 5- Plan ciągłości działania

VIII. Wykaz zabezpieczeń

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych – załącznik nr 6 -Wykaz zabezpieczeń.

2. W wykazie wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne, informatyczne i organizacyjne.

3. Wykaz jest aktualizowany po każdej analizie ryzyka

IX. Szkolenia

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO.

2. Za przeprowadzenie szkolenia odpowiada Administrator danych.

3. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

4. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.