Załącznik nr 1
do Zarządzenia Dyrektora Nr 18/18
z dnia 25 maja 2018 roku

Polityka Ochrony Danych Osobowych w Regionalnym Centrum Edukacji Zawodowej w Lubartowie

I. Wstęp

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora danych w Regionalnym Centrum Edukacji Zawodowej w Lubartowie 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. Inwentaryzacja danych

1. Administrator danych osobowych w Regionalnym Centrum Edukacji Zawodowej w Lubartowie dokonał inwentaryzacji przetwarzanych danych w formie określenia zbiorów danych. Inwentaryzacja danych ma formę opracowania pisemnego i stanowi dokument pt. "Rejestr zbiorów danych w Regionalnym Centrum Edukacji Zawodowej w Lubartowie, cz. I, II. "

2. Rejestr zbiorów składa się z dwóch części. W pierwszej części rejestru określono:

1) nazwę zbioru i jego wewnętrznie nadany numer;
2) wykaz aktywów biorących udział w czynnościach przetwarzania danych w zbiorze;
3) podstawę przetwarzania danych wynikającą z art. 6 lub/i art. 9 RODO;
4) decyzja administratora o opracowaniu lub nie opracowaniu rejestru czynności przetwarzania;
5) decyzja administratora o przeprowadzeniu lub nie przeprowadzaniu oceny skutków przetwarzania;
6) cele przetwarzania;
7) rodzaj i zakres danych;
8) odbiorcy danych znajdujących się w zbiorze;
9) opis operacji przetwarzania;
10) czas przechowywania danych.

W drugiej części Rejestru wskazano miejsce lokalizacji zbiorów, w tym zbiorów rozproszonych oraz formy zastosowanych zabezpieczeń fizycznych.

3. Wykaz zbiorów uwzględnia wszystkie dane osobowe, które są przetwarzane przez administratora i ewentualnie przez współadministratorów, które podlegają ochronie ze względu na ryzyko naruszenia praw i wolności osób fizycznych.

4. Administrator danych w celu oszacowania ryzyk przetwarzania danych osobowych dokonał audytu wewnętrznego. Wyniki audytu udokumentowane są w formie pisemnego opracowania w postaci kart, zawierających nazwę zbioru i wykaz aktywów biorących udział w procesie przetwarzania danych w konkretnym zbiorze.

5. W szkole została opracowana Polityka Zarządzaniem Ryzykiem w przetwarzaniu danych osobowych, określająca zasady szacowania skali ryzyka i prawdopodobieństwa jego wystąpienia, a tym samym istotności ryzyka.

6. Administrator, w uzgodnieniu z Inspektorem Ochrony Danych, opracował karty zawierające analizę ryzyka dla poszczególnych operacji przetwarzania danych szczególnej kategorii.

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 Jednolity rzeczowym wykazie akt, zatwierdzonym przez Archiwum Państwowe w Lublinie;

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

   5) osoby, których dane osobowe są przetwarzane zostały poinformowane o funkcji IOD i przekazano jego 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 w kolumnie " Cele przetwarzania" w Rejestrze Zbiorów Danych Osobowych.

3. Wzory klauzul informacyjnych znajdują się w Szkolnej dokumentacji ochrony danych – Klauzule Informacyjne.

IV. Upoważnienia

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

2. Administrator rejestruje wydane upoważnienia do przetwarzania danych oraz ich cofnięcia w Księdze Upoważnień. Imienne upoważnienia umieszczane są w aktach osobowych poszczególnych pracowników.

3. Każda osoba składa pisemne oświadczenie poufności. Oświadczenie o poufności umieszcza się w aktach osobowych pracowników lub dołącza się do umowy powierzenia.

4. Osoba upoważniona może przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.

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

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

7. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych w formie dokumentu - Ewidencja osób upoważnionych do przetwarzania danych osobowych.

V. 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:

1) dokonano opisu planowanych operacji przetwarzania i celów przetwarzania – opracowanie w dokumencie – Rejestr zbiorów danych osobowych;
2) określono zagrożenia we wszystkich aktywach biorących udział w procesie przetwarzania;
3) dokonano oceny ryzyk, zgodnie z zasadami wskazanymi w Polityce Zarządzania Ryzykiem;
4) sporządzono mapę ryzyk ze wskazaniem istotności ryzyka;
5) zaplanowano środki techniczne, organizacyjne i informatyczne dla ryzyk przekraczających istotność powyżej 4.

VI. Instrukcja postępowania z incydentami

Instrukcja 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 lub Inspektora 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 zainfekowaniem, 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 niebezpieczeństwa 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 wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze – dokument : 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.

VII. Regulamin Ochrony Danych

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania - załącznik 3 do Zarządzenia Dyrektora z dnia 25.05.2018 r. - Regulamin Ochrony Danych Osobowych

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania – załącznik 4 do Zarządzenia Dyrektora Nr18/18 z dnia 25.05.2018 r. - Oświadczenie poufności

VIII. 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 – dokument: "Plan ciągłości działania"

IX. Wykaz zabezpieczeń

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych –dokument: Wykaz zabezpieczeń.

2. W wykazie wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne, informatyczne i organizacyjne – dokument: Wykaz zabezpieczeń.

3. Wykaz jest aktualizowany.

X. 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. Administrator dokonał szkolenia wszystkich pracowników szkoły w formie e- szkolenia.

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

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

Lubartów, 25 maja 2018 r. .....

(podpis Administratora)