POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH w Zespole Szkół Technicznych "MECHANIK" w Jeleniej Górze

Administrator
w Zespole Szkół Technicznych
"MECHANIK"
w Jeleniej Górze

Wstęp

Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz postanowienia 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), w celu zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się następujące procedury.

Rozdział 1

Postanowienia ogólne

§ 1.

Ilekroć w dokumencie jest mowa o:

1) **rozporządzeniu** – rozumie się przez to 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);
2) **danych osobowych** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”). Możliwa do zidentyfikowania osoba fizyczna to osoba, 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;
3) **zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest

scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

4) **przetwarzaniu danych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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;
5) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
6) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
7) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
8) **administratorze danych** – rozumie się przez to Zespół Szkół Technicznych "MECHANIK" w Jeleniej Górze ul. Obrońców Pokoju 10;
9) **zgodzie osoby, której dane dotyczą** – oznacza to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
10) **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 postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
11) **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;

12) **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;

13) **ograniczeniu przetwarzania** – należy przez to rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

14) **profilowaniu** – oznacza to dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

15) **pseudonimizacji** – oznacza to 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;

16) **podmiocie przetwarzającym** – oznacza to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

17) **naruszeniu ochrony danych osobowych** – oznacza to naruszenie bezpieczeństwa 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;

18) **dane dotyczące zdrowia** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia.

Rozdział 2
Administrator danych
§ 1.

Administrator danych w szczególności:

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
2. Prowadzi rejestr czynności przetwarzania.
3. Wyznacza Inspektora Ochrony Danych (IOD).

Rozdział 3
Środki techniczne i organizacyjne
§ 3.

W celu ochrony danych spełniono wymogi, o których mowa w rozporządzeniu, w szczególności:

a) przestrzeganie postanowień rozporządzenia;
b) pozyskiwanie dobrowolnej zgody na przetwarzanie danych osoby, której dane dotyczą art 7 rozporządzenia - załącznik 1;
c) przekazywanie informacji osobom, od których zbierane są dane i której dane dotyczą art 13 rozporządzenia - załącznik nr 2
d) przeprowadzono ocenę skutków dla ochrony danych - art 35 rozporządzenia, zgodnie z załącznikiem nr 3,
e) przeprowadzono analizę ryzyka w stosunku do zasobów biorących udział w poszczególnych procesach zgodnie z załącznikiem nr 4,
f) do przetwarzania danych zostały dopuszczone wyłącznie osoby upoważnione - wzór upoważnienia - załącznik nr 5, przez administratora danych - rejestr osób upoważnionych - załącznik nr 6;
g) czynności przetwarzania danych osobowych rejestrowane są w rejestrze - art 30 rozporządzenia według załącznika nr 7

h) w przypadku powierzenia przetwarzania danych w imieniu Administratora podmiotowi przetwarzającemu, przetwarzanie odbywa się na podstawie umowy - wzór umowy załącznik nr 11;
i) została opracowana i wdrożona niniejsza polityka bezpieczeństwa.

§ 2.

W celu ochrony danych osobowych stosuje się następujące środki ochrony fizycznej danych osobowych:

a) zbiory danych osobowych przechowywane są w komputerach oraz (wersja papierowa) w zamykanych biurkach, szafach, szafach metalowych o podwyższonej odporności ogniowej >= 30 min, w pomieszczeniach zabezpieczonych zamykanymi na klucz drzwiami zwykłymi;
b) dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, objęty jest systemem kontroli dostępu;
c) dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych;
d) dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych, przez całą dobę jest nadzorowany przez służbę ochrony;
e) archiwalne zbiory danych osobowych przechowywane są w regałach w zamkniętym pomieszczeniu;
f) kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętym sejfie;
g) pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą gaśnicy proszkowej;
h) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób ręczny i mechaniczny za pomocą niszczarek dokumentów i przekazywane do firmy utylizującej dokumenty.

§ 5.

W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) komputery służące do przetwarzania danych osobowych nie są połączone z lokalną siecią komputerową;
b) zastosowano urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania;
c) dostęp do zbioru danych osobowych, który przetwarzany jest na wszystkich wydzielonych stacjach komputerowych/komputerach przenośnych, zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła;
d) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
e) w używanych programach zastosowany jest system mechanizmu wymuszający okresową zmianę haseł;
f) zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji;
g) dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia;
h) zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej;
i) zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity;
j) § 6. W celu ochrony danych osobowych stosuje się następujące środki ochrony w ramach narzędzi programowych i baz danych:
k) wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;
l) zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;
m) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
n) zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych;

o) zastosowano kryptograficzne środki ochrony danych osobowych;
p) stosować należy wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;
q) zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

§ 7.

W celu ochrony danych osobowych stosuje się następujące środki organizacyjne:

a) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
b) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego;
c) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
d) monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;
e) kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

Rozdział 4
Ocena skutków dla ochrony danych

§ 1.

Administrator dokonuje ocenę skutków dla ochrony danych na podstawie danych przekazanych z wykorzystaniem załącznika nr 3 przez osoby dokonujące procesu przetwarzania danych - art 35 rozporządzenia.

§ 2.

Ocena skutków ryzyka jest przeprowadzana według załącznika nr 4. Przy każdorazowej istotnej zmianie procesu przetwarzania danych osobowych, np. zmiana sposobu przetwarzania danych należy wykonać ocenę skutków ryzyka.

§ 3.

Ocenę skutków ryzyka należy przeprowadzić wraz z analizą ryzyka nie rzadziej niż raz w roku w stosunku do procesów, które w wyniku pierwszej oceny wykazały wysokie ryzyko dla praw i wolności osób, których dane dotyczą.

Rozdział 5
Procedura analizy ryzyka i plan postępowania z ryzykiem

§ 1.

Analizę ryzyka dla zasobów biorących udział w procesach przeprowadza każdorazowo pracownik upoważniony przez administratora danych lub administrator danych samodzielnie z wykorzystaniem załącznika nr 3.

§ 2.

Analiza ryzyka jest przeprowadzana nie rzadziej niż raz w roku i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.

§ 3.

Na podstawie wyników przeprowadzonej analizy ryzyka, wskazani przez administratora danych pracownicy wdrażają sposoby postępowania z ryzykiem.

§ 4.

Każdorazowo administrator danych wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą rozpatrywane jako pierwsze.

§ 5.

Administrator danych nie może zlekceważyć ryzyk, których wartość przekracza 6 punktów zgodnie z załącznikiem nr 4 lub ryzyka w stosunku do zasobu, biorącego udział w procesie wysokiego ryzyka zgodnie z wynikiem załącznika nr 4.

Rozdział 6
Procedura współpracy z podmiotami zewnętrznymi

§ 1.

Nie rzadziej niż raz w roku oraz każdorazowo przed zawarciem umowy powierzenia przetwarzania danych osobowych administrator danych weryfikuje zgodność z rozporządzeniem- art 28 wszystkich podmiotów przetwarzających, z których usług korzysta lub ma zamiar skorzystać.

§ 2.

Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych zgodnie z załącznikiem nr 11.

Rozdział 7
Procedura domyślnej ochrony danych

§ 1.

Administrator danych w przypadku zamiaru rozpoczęcia przetwarzania danych osobowych w nowym procesie przeprowadza analizę ryzyka w stosunku do tego procesu - art 25 rozporządzenia.

§ 2.

W każdym przypadku tworzenia nowego produktu lub usług administrator danych uwzględnia prawa osób, których dane dotyczą, na każdym kluczowym etapie jego projektowania i wdrażania.

Rozdział 8
Procedura zarządzania incydentami

§ 1.

W każdym przypadku naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

§ 2.

Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godz. od identyfikacji naruszenia - wzór raportu załącznik nr 9.

§ 3.

Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, przez zamieszczenie stosownego komunikatu zgodnie z załącznikiem nr 8 na swojej stronie internetowej - służbowa poczta e mail, poza przypadkami określonymi w art 34 rozporządzenia.

§ 4.

Administrator danych dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych - wzór rejestru naruszeń - załącznik nr 10.

Rozdział 8
Procedura realizacji praw osób

§ 1.

Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w rozporządzeniu administrator danych rozpatruje indywidualnie.

§ 2.

Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:

a) prawo dostępu do danych,
b) prawo do sprostowania danych,
c) prawo do usunięcia danych,
d) prawo do przenoszenia danych,
e) prawo do sprzeciwu wobec przetwarzania danych,
f) prawo do niepodlegania decyzjom oparty wyłącznie na profilowaniu.

§ 3.

W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

§ 4.

Administrator danych odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów rozporządzenia, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z rozporządzenia.

Rozdział 9
Procedura odbierania zgód oraz informowania osób

§ 1.

W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, zgodnie z załącznikiem nr 2.

§ 2.

W każdym przypadku pobierania danych z innych źródeł niż osoba, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, niezwłocznie, jednak nie później niż przy pierwszym kontakcie z osobą, której dane dotyczą, zgodnie z załącznikiem nr 2.

§ 3.

W każdym przypadku odbierania zgody od osoby, której dane dotyczą, korzysta się z klauzul zgody zgodnie z załącznikiem nr 1. - *art. 7 oraz 13 i 14 rozporządzenia.*

7

Rozdział 10
Postanowienia końcowe

§ 1.

Wszelkie zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych - załącznik nr 5, ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą - oświadczenie o zachowaniu poufności i zapoznaniu się z przepisami - załącznik nr 13.

§ 2.

Upoważnienia do przetwarzania danych Administrator odwołuje w przypadkach naruszenia przepisów bezpieczeństwa przetwarzania danych osobowych oraz na wniosek osób upoważnionych

§ 3.

Dokument niniejszy obowiązuje od dnia jego zatwierdzenia przez administratora.

Załączniki:

Załącznik nr 1 - Zgoda na przetwarzanie danych osobowych
Załącznik nr 2 - Informacja dla osób, których dane dotyczą
Załącznik nr 3 - Ankieta do oceny skutków przetwarzania danych
Załącznik nr 4 - Ocena skutków wystąpienia ryzyka
Załącznik nr 5 - Upoważnienie osób do przetwarzania danych osobowych
Załącznik nr 6 - Rejestr osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 7 - Rejestr czynności przetwarzania
Załącznik nr 8 - Komunikat naruszenia ochrony danych osobowych
Załącznik nr 9 - Raport o naruszeniu ochrony danych osobowych
Załącznik nr 10 - Rejestr naruszeń ochrony danych osobowych
Załącznik nr 11 - Umowa do przetwarzania danych osobowych
Załącznik nr 12 - Unieważnienie upoważnienia do przetwarzania danych osobowych
Załącznik nr 13 - Oświadczenie o zachowaniu poufności i zapoznaniu się z przepisami