Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Liceum Ogólnokształcącym Nr II im. Joachima Chreptowicza w Ostrowcu Świętokrzyskim

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 niniejszy zestaw procedur w Liceum Ogólnokształcącym Nr II im. Joachima Chreptowicza w Ostrowcu Świętokrzyskim.

Rozdział 1

Podstawa prawna

§ 1

Polityka Bezpieczeństwa Przetwarzania Danych Osobowych została przygotowana w oparciu o:

1) Konstytucję Rzeczypospolitej Polskiej (art. 47 i 51 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.);
2) ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych;
3) 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), dalej jako „RODO”;
4) ustawę z dnia 26 czerwca 1974 r. Kodeks pracy.

Definicje

§ 2

Podstawowymi pojęciami zastosowanymi w Polityce Bezpieczeństwa są:

1) **Administrator** lub **Szkoła** – Administrator Danych Osobowych, którym jest Liceum Ogólnokształcące Nr II im. Joachima Chreptowicza w Ostrowcu Świętokrzyskim, ul. Jana Rosłońskiego 1, 27-400 Ostrowiec Świętokrzyski;

2) **Administrator Systemu Informatycznego (ASI)** – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych;
3) **dane osobowe** – 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;
4) **Inspektor Ochrony Danych (IOD) –** osoba wyznaczona przez Administratora i zgłoszona do rejestru organu nadzorczego, odpowiedzialna za bezpieczeństwo danych osobowych w formie papierowej oraz przetwarzanie we wskazanych systemach informatycznych;
5) **Instrukcja** – Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Liceum Ogólnokształcącym Nr II im. Joachima Chreptowicza w Ostrowcu Świętokrzyskim;
6) **naruszenie ochrony danych osobowych** – 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;
7) **odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostka 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;
8) **osoba upoważniona** – osoba posiadająca upoważnienie wydane przez Administratora (lub osobę uprawnioną przez niego) i dopuszczona jako użytkownik do przetwarzania danych osobowych w formie elektronicznej (w systemie informatycznym) i papierowej w zakresie wskazanym w upoważnieniu;
9) **państwo trzecie** – państwo nienależące do Unii Europejskiej lub Europejskiego Obszaru Gospodarczego;
10) **podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

11) **Polityka Bezpieczeństwa** – niniejsza Polityka Bezpieczeństwa Przetwarzania Danych Osobowych, obowiązująca w Liceum Ogólnokształcącym Nr II im. Joachima Chreptowicza w Ostrowcu Świętokrzyskim;
12) **profilowanie** – dowolna forma 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;
13) **przetwarzanie danych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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;
14) **sieć publiczna** – sieć telekomunikacyjna niebędąca siecią wewnętrzną, służąca do świadczenia usług telekomunikacyjnych w rozumieniu ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne;
15) **sieć telekomunikacyjna** – urządzenia telekomunikacyjne zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną w rozumieniu ustawy Prawo telekomunikacyjne;
16) **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, zastosowanych w celu przetwarzania danych;
17) **środki techniczne i organizacyjne** – środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
18) **teletransmisja** – przesyłanie informacji za pomocą sieci telekomunikacyjnej;
19) **UODO –** Urząd Ochrony Danych Osobowych;
20) **użytkownik systemu** – osoba upoważniona do przetwarzania danych osobowych w systemie. Użytkownikiem może być osoba zatrudniona w szkole, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w szkole;
21) **zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych, zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

22) **zbiór danych** – uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie; zbiory danych określone są w załączniku nr 10;
23) **zgoda osoby, której dane dotyczą** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Rozdział 2

Administrator danych osobowych

§ 3

Administratorem danych osobowych jest Liceum Ogólnokształcące Nr II im. Joachima Chreptowicza w Ostrowcu Świętokrzyskim.

§ 4

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, Administrator:
   1) wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z prawem oraz możliwością wykazania tej zgodności. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane;
   2) zapewnia wymagane zaangażowanie pracowników w utrzymanie poziomu bezpieczeństwa informacji, w tym ochrony danych osobowych, które przetwarza Administrator;
   3) określa kierunki rozwoju zarządzania bezpieczeństwem informacji, w tym ochroną danych osobowych, przy jednoczesnym spełnieniu wszelkich wymogów obowiązującego prawa oraz zagwarantowaniu sprawnego funkcjonowania Administratora;
   4) identyfikuje i obniża katalog ryzyk związanych z bezpieczeństwem informacji, w tym ochroną danych osobowych;
   5) prowadzi rejestr czynności przetwarzania;
   6) wyznacza Inspektora Ochrony Danych (IOD), o czym zawiadamia Prezesa Urzędu Ochrony Danych Osobowych;
   7) wdraża Politykę Bezpieczeństwa Przetwarzania Danych Osobowych.
2. Ochronie podlegają w szczególności:
   1) dane osobowe przetwarzane przez Administratora niezależnie od ich formy i nośnika;
   2) sprzęt wykorzystywany do przetwarzania, przesyłania i przechowywania danych osobowych u Administratora;

3) pomieszczenia, w których znajduje się kluczowy sprzęt informatyczny zawierający dane osobowe (np. serwerownia);
4) dokumenty zawierające dane osobowe;
5) oprogramowanie wykorzystywane u Administratora;
6) pozostałe mienie wykorzystywane przez Administratora lub będące jego własnością;
7) informacje, których właścicielem są kontrahenci lub jednostki zewnętrzne współpracujące z Administratorem – w ramach tej współpracy.

Rozdział 3

Cele i zasady funkcjonowania Polityki Bezpieczeństwa

§ 5

1. Polityka Bezpieczeństwa w Szkole ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tj.:
   1) naruszeń danych osobowych rozumianych jako prywatne dobro powierzone Szkole;
   2) naruszeń przepisów prawa oraz innych regulacji;
   3) utraty lub obniżenia reputacji Szkoły;
   4) strat finansowych ponoszonych w wyniku nałożonych kar;
   5) zakłóceń organizacji pracy spowodowanych nieprawidłowym działaniem systemów.
2. Procedurę związaną z naruszeniem danych osobowych określa treść niniejszej Polityki Bezpieczeństwa oraz załączniki nr 8, 9, 11 i 12.
3. Administrator wyznacza Administratora Systemu Informatycznego (ASI), który:
   1) zarządza bezpieczeństwem przetwarzania danych osobowych w systemie informatycznym zgodnie z wymogami prawa i dokumentami wewnętrznymi z zakresu ochrony danych osobowych obowiązującymi w Szkole;
   2) doskonali i rozwija metody zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem;
   3) przydziela identyfikatory użytkownikom systemu informatycznego oraz zaznajamia ich z procedurami ustalania i zmiany haseł dostępu;
   4) nadzoruje prace związane z rozwojem, modyfikacją, serwisowaniem i konserwacją systemu;
   5) zapewnia bezpieczeństwo wewnętrznego i zewnętrznego obiegu informacji w sieci i zabezpieczenie łączy zewnętrznych;
   6) prowadzi nadzór nad archiwizacją zbiorów danych oraz zabezpiecza elektroniczne nośniki informacji zawierających dane osobowe.

4. Dyrektor Szkoły upoważniając pracownika zobowiązuje go do:
   1) ochrony prawa do prywatności osób fizycznych powierzających Szkole swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w Polityce Bezpieczeństwa i Instrukcji;
   2) zapoznania się z zasadami określonymi w Polityce Bezpieczeństwa i Instrukcji oraz złożenia oświadczenia o znajomości tych przepisów.

Środki techniczne i organizacyjne

§ 6

1. Przetwarzanie danych osobowych może odbywać się wyłącznie w obszarach do tego celu przeznaczonych. Wykaz pomieszczeń, w których dopuszczalne jest przetwarzanie danych osobowych, stanowi załącznik nr 6.
2. Dostęp do pomieszczeń, w których przetwarzane są dane osobowe, oraz do pomieszczeń, w których znajdują się serwery baz danych lub przechowywane są kopie zapasowe, jest zabezpieczony przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w tym obszarze jest możliwe tylko w obecności osoby upoważnionej do przetwarzania danych osobowych. Wejście do tego obszaru jest zabezpieczone.

§ 7

1. Przetwarzać dane osobowe może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych (załącznik nr 5).
2. Administrator prowadzi wykaz osób upoważnionych do przetwarzania danych osobowych (załącznik nr 7).
3. Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła.
4. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora.
5. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.

§ 8

1. W celu ochrony danych osobowych stosuje się politykę czystego biurka i czystego ekranu.

2. W przypadku dłuższej nieobecności przy stanowisku pracy lub po jej zakończeniu pracownik jest zobowiązany do umieszczenia wszelkich dokumentów i nośników zawierających dane osobowe w bezpiecznym miejscu, np. zamykanej szafce. Nie należy również dokumentów i nośników pozostawiać w łatwo dostępnych miejscach.
3. Niepotrzebne dokumenty powinny być niezwłocznie niszczone za pomocą niszczarki.

§ 9

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

1) komputery służące do przetwarzania danych osobowych nie są połączone z lokalną siecią komputerową;
2) w przypadku opuszczenia stanowiska pracy pracownik jest zobowiązany do wylogowania się z aplikacji lub zablokowania pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu lub aplikacji osoby nieupoważnionej zgodnie z procedurą wynikającą z Instrukcji (załącznik nr 13);
3) stosuje się urządzenia typu UPS lub listwy przeciwprzepięciowe, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania;
4) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
5) stosuje się system rejestracji dostępu do systemu, w którym są przetwarzane dane osobowe;
6) dostęp do środków teletransmisji zabezpieczony jest za pomocą mechanizmów uwierzytelnienia;
7) stosuje się środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity;
8) używa się zapory sieciowej (*firewall*) do ochrony dostępu do sieci komputerowej.

§ 10

W celu ochrony danych osobowych stosuje się środki ochrony w ramach narzędzi programowych i baz danych:

1) pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;
2) umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;

3) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
4) środki systemowe pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych, dla poszczególnych użytkowników systemu informatycznego;
5) mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych;
6) zainstalowane są wygaszacze ekranu wraz z blokadą dostępu na stanowiskach, na których przetwarzane są dane osobowe;
7) stosuje się mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Rozdział 4

Procedura DPIA *(Data Protection Impact Assessment)*

§ 11

Ocenę skutków dla ochrony danych osobowych (DPIA) przeprowadza każdorazowy właściciel procesu wskazany przez Administratora z wykorzystaniem załącznika nr 1, w stosunku do procesów, które po przeprowadzonej analizie ryzyka wykazują wysokie ryzyko dla praw i wolności osób, których dane dotyczą.

§ 12

1. Jeżeli dany rodzaj przetwarzania danych osobowych, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (DPIA).
2. DPIA jest przeprowadzana wraz z analizą ryzyka nie rzadziej niż raz w roku w stosunku do procesów, które wykazują wysokie ryzyko dla praw i wolności osób, których dane dotyczą.

Rozdział 5

Procedura zarządzania ryzykiem i plan postępowania z ryzykiem

§ 13

Procedurę zarządzania ryzykiem i analizę ryzyka dla zasobów biorących udział w procesach przeprowadza każdorazowy właściciel procesu wskazany przez Administratora lub Administrator samodzielnie, z wykorzystaniem załącznika nr 2.

§ 14

Analiza ryzyka stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem.

§ 15

Na podstawie wyników przeprowadzonej analizy ryzyka, wskazani przez Administratora właściciele procesów lub Administrator wdrażają sposoby postępowania z ryzykiem.

§ 16

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

§ 17

Administrator nie może zlekceważyć ryzyk, których wartość przekracza 210 punktów zgodnie z załącznikiem nr 2 lub ryzyka w stosunku do zasobu, biorącego udział w procesie wysokiego ryzyka zgodnie z wynikiem DPIA, określonym według załącznika nr 1.

Rozdział 6

Procedura współpracy z podmiotami zewnętrznymi

§ 18

Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych (załącznik nr 3).

Rozdział 7

Procedura domyślnej ochrony danych

§ 19

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

Rozdział 8

Procedura zarządzania incydentami

§ 20

W każdym przypadku naruszenia ochrony danych osobowych Administrator weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych na podstawie procedury określonej jako Instrukcja postępowania w sytuacji naruszenia danych (załącznik nr 14).

§ 21

Administrator w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, w miarę możliwości nie później niż w ciągu 72 godz. od identyfikacji naruszenia.

§ 22

Administrator zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, chyba że zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.

§ 23

1. Administrator dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych i sporządza raport zgodnie z załącznikiem nr 8.
2. Administrator prowadzi rejestr naruszeń bezpieczeństwa zgodnie z załącznikiem nr 9.

Rozdział 9

Procedura realizacji praw osób

§ 24

Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w RODO, Administrator rozpatruje indywidualnie.

§ 25

Administrator niezwłocznie realizuje następujące prawa osób, których dane dotyczą:

1) prawo dostępu do danych,
2) prawo do sprostowania danych,
3) prawo do usunięcia danych,

4) prawo do przenoszenia danych,
5) prawo do sprzeciwu wobec przetwarzania danych,
6) prawo do niepodlegania decyzjom opartym wyłącznie na profilowaniu.

§ 26

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

§ 27

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

§ 28

Szczegółowa procedura realizacji praw osób, których dane dotyczą, stanowi załącznik nr 15.

Rozdział 10

Procedura odbierania zgód oraz informowania osób

§ 29

W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, Administrator w zwięzłej, przejrzystej formie i zrozumiałym językiem informuje osobę, której dane dotyczą, zgodnie z załącznikiem nr 4.

§ 30

W każdym przypadku pobierania danych z innych źródeł niż osoba, której dane dotyczą, Administrator informuje niezwłocznie osobę, której dane dotyczą, jednak nie później niż przy pierwszym kontakcie z osobą, której dane dotyczą, zgodnie z załącznikiem nr 4a.

§ 31

W każdym przypadku odbierania zgody od osoby, której dane dotyczą, korzysta się z wzoru zgody na przetwarzanie danych osobowych, określonej odpowiednio w załącznikach nr 16, nr 16a, nr 22 lub nr 23.

Rozdział 11

Postanowienia końcowe

§ 32

Wszelkie zasady opisane w niniejszym dokumencie są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych, ze szczególnym uwzględnieniem dobra osób, których dane dotyczą.

§ 33

Dokument niniejszy obowiązuje od dnia jego zatwierdzenia przez Administratora.

…….

administrator danych osobowych

Wykaz załączników:

1) arkusz DPIA (załącznik nr 1),
2) wzór umowy powierzenia przetwarzania danych osobowych (załącznik nr 2),
3) wzór klauzuli informacyjnej (załączniki nr 3 i 3a),
4) wzór upoważnienia do przetwarzania danych osobowych (załącznik nr 4),
5) wykaz pomieszczeń, w których dopuszczalne jest przetwarzania danych (załącznik nr 5),
6) ewidencja nadanych upoważnień (załącznik nr 6),
7) wzór raportu z naruszenia ochrony danych osobowych (załącznik nr 7),
8) rejestr naruszeń bezpieczeństwa (załącznik nr 8),
9) zbiory danych (załącznik nr 9),
10) wzór zgłoszenia naruszenia do UODO (załącznik nr 10),
11) wzór komunikatu o naruszeniu ochrony danych osobowych (załącznik nr 11),
12) Instrukcja Zarządzania Systemem Informatycznym (załącznik nr 12),
13) instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych (załącznik nr 13),
14) procedura realizacji praw osób, których dane dotyczą (załącznik nr 14),
15) wzór zgody na przetwarzanie danych osobowych (załączniki nr 15 i 15a),
16) procedura nadawania, zmiany lub wycofania upoważnień do przetwarzania danych osobowych (załącznik nr 16),
17) wzór polecenia dotyczącego uprawnień do systemów informatycznych (załącznik nr 17),
18) rejestr żądań udostępnień danych osobowych (załącznik nr 18),
19) rejestr kategorii czynności przetwarzania (załącznik nr 19),
20) opis stosowanych środków bezpieczeństwa (załącznik nr 20),
21) wzór zgody na publikację wizerunku i nazwiska (załącznik nr 21),
22) wzór zgody na przetwarzanie numeru telefonu i adresu poczty elektronicznej (załącznik nr 22).