Polityka Ochrony Danych Osobowych

w Powiślańskiej Szkole Wyższej

Spis treści:

§ 1

WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, Dz.Urz.UE L z 2016 r., Nr 119, s.1 (RODO).

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

DEFINICJE:

Administrator (danych) - Administratorem Danych Osobowych jest Powiślańska Szkoła Wyższa, ul. 11 Listopada 29, 82 – 500 Kwidzyn. Administrator jest reprezentowany przez Rektora prof. dr hab. Krystynę Strzała.

Administrator danych osobowych mając na uwadze znaczenie zasad bezpieczeństwa w zakresie przetwarzania danych osobowych, kierując się zasadą ochrony podstawowych praw i wolności osób fizycznych, a w szczególności ich prawem do należytej ochrony danych osobowych oraz w celu zapewnienia zgodności procedur przetwarzania tych danych z wymaganiami prawa, a także mając na uwadze znaczenie ochrony dobrego imienia jednostki, ustanawia niniejszym Politykę ochrony danych osobowych tj. zasady oraz zabezpieczenia stosowane podczas przetwarzania danych osobowych w Uczelni.

Mając na uwadze powyższe, Administrator zobowiązuje się przestrzegać podstawowych zasad dotyczących przetwarzania danych osobowych oraz wykazania ich przestrzegania (zasada rozliczalności) - do których należą:

a. Zasada przetwarzania danych osobowych zgodnie z prawem w sposób rzetelny i przejrzysty.
b. Zasada ograniczonego celu która oznacza, że dane osobowe mogą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz ich nieprzetwarzane w sposób niezgodny z tymi celami.
c. Zasada minimalizmu, która oznacza, że dane osobowe mogą być przetwarzane wyłącznie w niezbędnym zakresie i wyłącznie do celów dla których są przetwarzane.
d. Zasada prawidłowości, zgodnie z którą dane przetwarzane przez Administratora powinny być aktualne i poprawne, zaś dane osobowe które są nieprawidłowe powinny być niezwłocznie usunięte lub sprostowane.
e. Zasada ograniczonego przetwarzania, która oznacza, że dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą i przez okres nie dłuższy niż niezbędny do celów, dla których dane te są przetwarzane.
f. Zasada integralności i poufności, które wymagają aby dane osobowe były przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym należytą ochronę przez niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz ich przypadkową utratą, zniszczeniem lub uszkodzeniem za pomocą odpowiednich środków technicznych lub organizacyjnych.

Anonimizacja- nieodwracalna zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych poprzez pozbawienie ich cech identyfikacyjnych. Na podstawie danych, które uległy procesowi anonimizacji nie jest możliwe zidentyfikowanie osób fizycznych, których pierwotnie dane osobowe dotyczyły.

Dane osobowe - oznaczają wszelkie 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, adresy IP, identyfikatory plików cookie, dane o lokalizacji, identyfikator

internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Incydent bezpieczeństwa informacji- jest to przypadkowe lub niezgodne z prawem zdarzenie prowadzące do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi przetwarzającemu w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Naruszenie ochrony danych osobowych - incydent naruszenia bezpieczeństwa danych osobowych prowadzący do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych związany z ryzkiem naruszenia praw lub wolności osób, których dotyczą.

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.

Przetwarzanie danych osobowych – oznacza każdą czynność wykonywaną na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany np.:
- zbieranie,
- utrwalanie,
- organizowanie,
- porządkowanie,
- przechowywanie,
- adaptowanie lub modyfikowanie danych,
- pobieranie,
- przeglądanie,
- wykorzystywanie,
- ujawnianie poprzez przesłanie,
- rozpowszechnianie lub innego rodzaju udostępnianie,
- dopasowywanie,
- łączenie,
- ograniczanie,
- usuwanie lub niszczenie danych.

Podmiot przetwarzający- podmiot, który w imieniu Administratora przetwarza dane osobowe na podstawie umowy powierzenia. Umowa powierzenia powinna określać m.in.: przedmiot, cel, czas i zakres przetwarzania, a także rodzaj przetwarzanych danych.

Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

RODO - 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, Dz.Urz.UE L z 2016 r., Nr 119, s.1).

Szczególne kategorie danych osobowych – dane osobowe, które ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące naturalnego życie seksualne osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

Profilowanie – jest dowolną formą zautomatyzowanego przetwarzania danych osobowych, która 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.

Zgoda na przetwarzanie danych osobowych - oznacza dobrowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Na Administratorze ciąży obowiązek odpowiedniego udokumentowania faktu udzielenia zgody dla celów dowodowych.

§ 2

OCENA SKUTKÓW (ANALIZA RYZYKA)

1. Opis operacji przetwarzania (inwentaryzacja aktywów)

W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. Dane te w postaci zbiorów (kategorii osób) zostały wykazane w załączniku 01a Wykaz zbiorów danych osobowych

Opis zbiorów (kategorii osób) powinien obejmować takie informacje, jak:

a) nazwę zbioru (opis kategorii osób)
b) opis celów przetwarzania
c) charakter, zakres, kontekst danych osobowych
d) odbiorcy danych
e) funkcjonalny opis operacji przetwarzania
f) aktywa służące do przetwarzania danych osobowych (Informacje, Programy, Systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy,
Outsourcing) – załącznik 02b Lista potencjalnych aktywów
g) informacja o konieczności wpisu do rejestru czynności przetwarzania
h) informacja o konieczności przeprowadzenia oceny skutków dla zbioru

2. Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO)

W ramach przeprowadzenia analizy ryzyka w zakresie przetwarzania danych osobowych Administrator jest zobowiązany do spełnienia wobec osób, których dane dotyczą obowiązków prawnych.

W szczególności Administrator zobowiązany jest zapewnić, że :

a) dane te są legalnie przetwarzane,
b) dane te są adekwatne w stosunku do celów przetwarzania,
c) dane te są przetwarzane przez określony czas (retencja danych),
d) wobec tych osób wykonano tzw. obowiązek informacyjny wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody),
e) opracowano zgody na przetwarzanie danych osobowych oraz klauzule informacyjne dla powyższych osób (załącznik: 01c – zgody na przetwarzanie danych osobowych i 01b Klauzule informacyjne),
f) istnieją umowy powierzenia z podmiotami przetwarzającymi zgodnie z załącznikiem 01g Umowa powierzenia (wykaz podmiotów przetwarzających prowadzony jest w załączniku 01f Rejestr umów powierzenia).

3. Analiza Ryzyka

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania (np. dla zbioru pracowników, zbioru studentów, dla procesu wysyłania informacji newsletter dla zapisanych odbiorców)

3.1. Definicje

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych,
2. Zagrożenie - potencjalne naruszenie (potencjalny incydent),
3. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia),
4. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

3.2 Wyznaczenie zagrożeń

1. Administrator jest odpowiedzialny za określenie listy zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania.
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów.
3. Wykaz przykładowych zagrożeń (załącznik 02c Lista potencjalnych zagrożeń).

3.3 Wyliczenie ryzyka dla zagrożeń

1. Administrator określa Prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania.
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A.
3. Administrator określa Skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne.
4. Proponowaną Skalę skutków prezentuje Tabela B.
5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: R = P * S.

Tabela A - PRAWDOPODOBIEŃSTWO	**POZIOM**

Bardzo wysokie	5
Wysokie	4
Średnie	3
Niskie	2
Bardzo niskie	1

Tabela B - Skutek	**Poziom**	**Opis**
Bardzo wysoki	5	Może nastąpić bezpowrotna utrata danych, praca przedsiębiorstwa zostaje zatrzymana do czasu przywrócenia właściwego funkcjonowania, duże straty finansowe
Wysoki	4	Praca przedsiębiorstwa może zostać wstrzymana do czasu usunięcia przyczyny, straty finansowe,
Średni	3	Praca przedsiębiorstwa jest zakłócona, należy przywrócić właściwy stan zabezpieczeń
Niski	2	Praca przedsiębiorstwa przebiega bez zakłóceń, mogą nastąpić straty finansowe w niewielkiej skali
Bardzo niski	1	Brak wpływu na funkcjonowanie przedsiębiorstwa

3.4 Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem
2. Proponowaną skalę Ryzyka prezentuje Tabela C

Tabela C – Macierz Ryzyka			SKUTKI				
			B. niski	Niski	Średni	Wysoki	B. wysoki
			1	2	3	4	5
Prawdopodobieństwo	B. wysokie	5	Ś	W	K	K	K
	Wysokie	4	Ś	W	W	K	K
	Średnie	3	N	Ś	W	W	K
	Niskie	2	N	N	Ś	W	W
	B. niskie	1	N	N	Ś	W	W

Poziom ryzyka:

N – od 1 do 4 - niski, poziom ryzyka akceptowalny, działania należy podjąć na podstawie nakładów potrzebnych do jego zmniejszenia

Ś – do 5 do 7 – średni, poziom ryzyka nieakceptowalny, działanie można jednak podjąć w późniejszym terminie pod warunkiem okresowej kontroli

W – od 8 do 15 – wysoki, poziom ryzyka nieakceptowalny, działanie można podjąć w późniejszym terminie, jednocześnie stale monitorując sytuację

K – od 16 do 25 – krytyczny, poziom nieakceptowalny, wymaga natychmiastowego działania.

3.5 Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń.
2. Działania obniżające ryzyko, które może zastosować Administrator:

a) Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie),

b) Unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji),

c) Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrivów z danymi wynoszonych poza firmę).

3. Wykaz przykładowych zabezpieczeń (załącznik - 02d Lista potencjalnych zabezpieczeń).
4. Analizę ryzyka przeprowadza się w specjalnym szablonie (programie), (załącznik - 02e Arkusz analizy ryzyka RODO).

3.6 Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne).

4. Plan postępowania z ryzykiem

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

§ 3

UPOWAŻNIENIA

1. Administrator odpowiada za nadawanie oraz anulowanie upoważnień do przetwarzania danych osobowych zgromadzonych w zbiorach papierowych oraz systemach informatycznych.
2. Administrator może powierzyć powyższe uprawnienie Inspektorowi Ochrony Danych.
3. Dział Kadr zobowiązany jest przekazać Administratorowi oraz Inspektorowi Ochrony Danych informację o nowo zatrudnionym pracowniku lub nawiązaniu współpracy na podstawie umowy cywilnoprawnej w związku z wykonywaniem której celowe i konieczne jest nadanie pracownikowi/zleceniobiorcy upoważnienia do przetwarzania danych w zbiorach papierowych oraz systemach informatycznych. Dział Kadr jest obowiązany wskazać zbiór danych osobowych oraz zakres upoważnienia, jakie jest niezbędne i konieczne celem wykonywania czynności służbowych lub zleconych.
4. Dział Kadr ma obowiązek niezwłocznego powiadomienia Administratora oraz Inspektora Ochrony Danych o fakcie wypowiedzenia umowy o pracę, rozwiązania umowy o pracę lub rozwiązaniu umowy o współpracy, a także o każdym innym zdarzeniu (np. zmiana zakresu obowiązków) – ze względu na które konieczne jest anulowanie lub zmiana zakresu upoważnienia do przetwarzania danych osobowych dla danego pracownika lub zleceniobiorcy.
5. Przetwarzanie danych osobowych przez pracownika lub zleceniobiorcę może odbywać się wyłącznie na podstawie i w zakresie przepisów prawa, w tym na podstawie pisemnego upoważnienia do przetwarzania danych osobowych lub polecenia służbowego wydanego i potwierdzonego przez Administratora lub Inspektora Danych Osobowych.
6. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie (załącznik - 01e Upoważnienie do przetwarzania danych osobowych).
7. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia.
8. Inspektor Ochrony Danych prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych (załącznik - 01d Ewidencja osób upoważnionych).

§ 4

INSTRUKCJA POSTĘPOWANIA Z NARUSZENIAMI / INCYDENTAMI

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

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu naruszenia/incydentu bezpośredniego przełożonego, Kanclerza lub Inspektora Ochrony Danych)

2. Do typowych podatności bezpieczeństwa danych osobowych należą:

a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów

b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych

c) 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:

a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)

b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)

c) 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 w przypadku powołania – IOD) prowadzi postępowanie wyjaśniające w toku, którego:

a) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,

b) inicjuje ewentualne działania dyscyplinarne,

c) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,

d) 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, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze – (załącznik - 03 Ewidencja naruszeń/incydentów).

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.

§ 5

REGULAMIN OCHRONY DANYCH OSOBOWYCH

1. Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania (załącznik - 04 Regulamin Ochrony Danych Osobowych).

2. Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania (załącznik - 04a Oświadczenie poufności pracownik/ dla osób realizujących inne zlecenia).

§ 6

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 Inspektor Danych Osobowych.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia za pomocą załącznika 05a Plan szkolenia RODO.
4. Materiały szkoleniowe dla uczestników szkolenia zostały opracowane wg załącznika 05b Szkolenie wewnętrzne RODO.
5. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania (załącznik - 04a Oświadczenie poufności).

§ 7

REJESTR CZYNNOŚCI PRZETWARZANIA

1. W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Administratora, wypełnia załącznik 06a Rejestr czynności prowadzony przez Administratora.
2. W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Podmiot przetwarzający, wypełnia załącznik 06b Rejestr czynności prowadzony przez Podmiot przetwarzający.

§ 8

AUDYTY

1. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. W tym celu Administrator stosuje procedurę audytów (załącznik- 07 Procedura audytu).

§ 9

PROCEDURA PRZYWRÓCENIA DOSTĘPNOŚCI DANYCH OSOBOWYCH I DOSTĘPU DO NICH W RAZIE INCYDENTU FIZYCZNEGO LUB TECHNICZNEGO (BCP)

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, opisane w załączniku - 08 Plan ciągłości działania.

§ 10

WYKAZ ZABEZPIECZEŃ

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych, opisane w załączniku Instrukcja zarządzania systemami informatycznymi/ Wykaz zabezpieczeń RODO. W instrukcji/wykazie wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne.
2. Instrukcja / wykaz jest aktualizowana po każdej analizie ryzyka / ocenie skutków.