Polityka Ochrony Danych Osobowych w Państwowej Wyższej Szkole Techniczno-Ekonomicznej im. ks. Bronisława Markiewicza w Jarosławiu

Wstęp

Państwowa Wyższa Szkoła Techniczno-Ekonomiczna im. ks. Bronisława Markiewicza w Jarosławiu jest Administratorem Danych Osobowych, a czynności z zakresu ochrony danych osobowych wykonuje Rektor PWSTE w Jarosławiu. Jest On zobowiązany do podejmowania wszelkich możliwych działań koniecznych do zapobiegania zagrożeniom związanym z przetwarzaniem danych osobowych.

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowanych przez Administratora w celu spełnienia wymagań Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz ustawy z 10 maja 2018 r. o ochronie danych osobowych (Dz.2018r. poz. 1000).

Celem niniejszej Polityki Ochrony Danych Osobowych jest wypełnienie założeń 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, dalej też zwane RODO). Stanowi ona zbiór wymogów, zasad i regulacji ochrony danych osobowych u Administratora danych osobowych.

REKTOR
prof. ucz. dr hab. Krzysztof Rejman

Spis treści

Rozdział 1

Postanowienia ogólne

§1

Definicje

Na użytek niniejszego dokumentu:

1. Polityka – „Polityka Ochrony Danych Osobowych w Państwowej Wyższej Szkole Techniczno-Ekonomicznej im. ks. Bronisława Markiewicza w Jarosławiu",
2. Dane osobowe – oznaczają 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. Zbiór danych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,
4. Administrator – osoba fizyczna lub prawa, organ publiczny, jednostka organizacyjna lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
5. Podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka organizacyjna lub inny podmiot, który w imieniu administratora przetwarza dane osobowe,
6. Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom 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 oraz wykonywanie innych zadań określonych w art. 39 RODO,
7. Ryzyko - wskaźnik stanu lub zdarzenia, które może prowadzić do strat. Jest ono proporcjonalne do prawdopodobieństwa wystąpienia tego zdarzenia i do wielkości strat, które może spowodować,
8. Przetwarzanie – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łącznie, ograniczanie, usuwanie lub niszczenie,
9. Odbiorca – każda 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 UE lub prawem państwa członkowskiego, nie są uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych osobowych mającymi zastosowanie do celów przetwarzania,
10. Zgoda osoby, której dane dotyczą – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie pisemnego oświadczenia lub

wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych,

11. Naruszenie ochrony danych osobowych (incydent) – 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.

§2

Polityka określa:

a) zasady na podstawie, których opiera się przetwarzanie danych osobowych oraz sposób uzyskiwania upoważnień oraz nadawania uprawnień do przetwarzania danych osobowych,
b) procedurę przeprowadzania analizy ryzyka oraz instrukcję postępowania w przypadku wystąpienia incydentu,
c) wykaz zbiorów danych osobowych ze wskazaniem podstaw prawnych przetwarzania, aktywów, celi przetwarzania, rodzajów i zakresów danych oraz odbiorców, opisu operacji przetwarzania, czasu przechowywania,
d) wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
e) wykaz zabezpieczeń stosowanych w celu ochrony danych osobowych;
f) Regulamin Ochrony Danych Osobowych,
g) Politykę kluczy,
h) sposób zapoznawania pracowników z nowelizacją przepisów (szkolenie wewnętrzne pracowników).

Rozdział 2

Inwentaryzacja danych. Zasady przetwarzania danych osobowych. Odpowiedzialność. Obowiązek informacyjny. Porozumienia i kontakty ze stronami zewnętrznymi.

§3

1. Dane osobowe wymagające ochrony zostały wykazane w załączniku do niniejszej Polityki (Załącznik nr 1 – Wykaz zbiorów danych osobowych).
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. Opis zbiorów obejmuje takie informacje, jak:
    a. nazwę zbioru;
    b. opis celów przetwarzania;
    c. charakter, zakres, kontekst, dokumentowane dane osobowe;
    d. odbiorcy;
    e. funkcjonalny opis operacji przetwarzania;

f. aktywa służące do przetwarzania danych osobowych;
g. informacja o konieczności przeprowadzania oceny skutków dla zbioru;
h. kategorię osób, której dane dotyczą;
i. dane administratora – osoby odpowiedzialnej za gromadzone dane;
j. planowane terminy usunięcia danych;
k. podstawa prawna przetwarzania.

§4

1. Administrator oraz podmiot przetwarzający zapewniają, że dane osobowe przetwarzane są zgodnie z poniższymi regułami:

a) zgodni z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zgodność z prawem, rzetelność i przejrzystość),
b) zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach (ograniczenie celu),
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych),
d) prawidłowe i w razie potrzeby uaktualniane (prawidłowość),
e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane, z wyjątkami wskazanymi w rozporządzeniu (ograniczenie przechowywania),
f) w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (integralność i poufność),
g) wobec osób, których dane osobowe są przetwarzane wykonano tzw. obowiązek informacyjny – prawo dostępu do danych, prawo przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu.

2. Administrator prowadzi rejestr czynności przetwarzania. Rejestr czynności stanowi równocześnie wykaz zbiorów danych osobowych Administratora (Załącznik nr 1).
3. Podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania.

§5

1. Do stosowania zasad określonych przez dokumenty Polityki zobowiązani są wszyscy pracownicy PWSTE w Jarosławiu, niezależnie od podstawy zatrudnienia oraz osoby wykonujące umowy cywilnoprawne, którzy w ramach obowiązków służbowych przetwarzają dane osobowe.
2. Każda osoba mająca dostęp do danych osobowych przetwarzanych w PWSTE w Jarosławiu jest zobowiązana do zapoznania się z niniejszym dokumentem.

§6

1. Administrator/podmiot przetwarzający odpowiada za nadawanie oraz anulowanie upoważnień do przetwarzania danych osobowych w zbiorach papierowych, systemach informatycznych.
2. Podmiot przetwarzający oraz każda osoba działająca z upoważnienia Administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenia Administratora, chyba, że wymaga tego przepis prawa.

3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych (kierowników/dyrektorów działów). Kierownicy jednostek organizacyjnych określają zakres kompetencji przetwarzania danych osobowych.
4. Upoważnienia określają zakres operacji na danych.
5. Upoważnienia powinny być przechowywane w aktach osobowych pracowników (ewentualnie w dokumentacji odpowiednich komisji), powinny być udostępniane tylko osobom upoważnionym oraz aktualizowane w przypadku zmiany zakresu obowiązków.
6. Upoważnienia mogą być wyjątkowo nadawane w formie poleceń, np. upoważnienie do przeprowadzenia kontroli, audytów, wykonania czynności służbowych.
7. Inspektor Ochrony Danych prowadzi ewidencję osób upoważnionych, w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja stanowi załącznik do niniejszej Polityki (Załącznik nr 2 –wzór Ewidencji osób upoważnionych. Ewidencja prowadzona jest w formie elektronicznej).

§7

1. Uprawnienia do przetwarzania danych osobowych w systemie informatycznym nadawane są na wniosek przełożonych (kierowników/dyrektorów działów) osób, które mają przetwarzać dane.
2. Kierownicy jednostek organizacyjnych działów określają systemy informatyczne, do których dostęp mają pracownicy ich działów oraz zakres kompetencji.
3. Uprawnienie, o którym mowa w pkt. 1 jest anulowane z chwilą zaprzestania przetwarzania danych osobowych przez osobę, której uprawnienie zostało nadane bądź z ustaniem zatrudnienia.

§8

1. Administrator pozyskując dane osobowe od osoby, której dotyczą jest zobowiązany podać jej następujące informacje:
    a) swoją tożsamość i dane kontaktowe,
    b) dane kontaktowe Inspektora Ochrony Danych,
    c) cele przetwarzania danych oraz podstawę prawną przetwarzania,
    d) jeżeli przetwarzanie danych osobowych związane jest z realizacją prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią – należy wskazać prawnie uzasadnione interesy,
    e) informację o odbiorcach danych osobowych lub o kategoriach odbiorców,
    f) w przypadkach gdy ma to zastosowanie – informacje o zamiarze przekazania danych do państwa trzeciego lub organizacji międzynarodowej,
    g) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
    h) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,
    i) informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (reguła ta ma zastosowanie do przetwarzania danych na podstawie zgody wyrażonej w jednym lub większej liczbie celów oraz przetwarzania danych wrażliwych na podstawie zgody osoby, której dane dotyczą),
    j) informację o prawie wniesienia skargi do organu nadzorczego,
    k) informację, czy podanie danych jest wymogiem ustawowym lub umownym lub warunkiem zwarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,

l) informacje o zautomatyzowanym podejmowaniu decyzji.

2. W przypadku, gdy Administrator pozyskuje dane osobowe z innego źródła niż osoba, której dane dotyczą, Administrator jest zobowiązany podać tej osobie wszystkie informację wymienione w pkt. 1 a dodatkowo: podać informację o źródle pochodzenia danych osobowych.
3. Informacje, o których mowa w pkt. 2 Administrator podaje w rozsądnym terminie po pozyskaniu danych, najpóźniej w ciągu miesiąca mając na uwadze konkretne okoliczności przetwarzania danych osobowych. W przypadku, gdy dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą administrator przekazuje dane najpóźniej przy pierwszej takiej komunikacji. Jeżeli planuje się ujawnić dane osobowe innemu odbiorcy najpóźniej przy pierwszym ich ujawnieniu.

§9

1. Dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane, przez okres nie dłuższy niż jest to niezbędne do celów, dla których dane te są przetwarzane. Dane osobowe mogą być przechowywane przez okres dłuższy, jeżeli będą przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów naukowych lub historycznych lub do celów statystycznych.
2. Dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.
3. Osoba, której dane dotyczą ma prawo żądać od Administratora sprostowania dotyczących jej danych, które są nieprawidłowe.
4. Osoba, której dane dotyczą ma prawo żądać od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć dane, jeśli zachodzi jedna z przesłanek:
   a) dane osobowe nie są już niezbędne dla celów, dla jakich zostały zebrane,
   b) osoba, której dane dotyczą cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania,
   c) osoba, której dane dotyczą wnosi sprzeciw na mocy przepisów prawa i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,
   d) dane osobowe były przetwarzane niezgodnie z prawem,
   e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego,
   f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.
5. Osoba, której dane dotyczą ma prawo żądać ograniczenia przetwarzania w następujących przypadkach:
   a) osoba, której dane dotyczą kwestionuje ich prawidłowość,
   b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą sprzeciwia się usunięciu danych,
   c) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą do ustalenia, dochodzenia lub obrony roszczeń,
   d) osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania.
6. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.
7. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

PR

§10

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło praw osób, których dane dotyczą.
2. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, wiążąc podmiot podmiot przetwarzający i administratora, określając przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.
3. W przypadku zawierania umów z firmami zewnętrznymi mającymi wpływ na funkcjonowanie kluczowych elementów systemu zarządzania bezpieczeństwem informacji zalecane jest zawarcie umowy powierzenia.

Rozdział 3

Procedura analizy ryzyka/ocena skutków

§11

1. Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić podczas przetwarzania danych osobowych.
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zinwentaryzowanych zbiorów (kategorii osób), aktywów oraz procesów przetwarzania.
3. Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.
4. Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru danych osobowych lub grupy zbiorów charakteryzujących się podobieństwem celów i sposobów przetwarzania.
5. W przypadku konieczności przeprowadzenia oceny skutków, (jeżeli rodzaj przetwarzania, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych), wymagane jest wykonanie następujących czynności:

a) Systematyczny opis planowanych operacji przetwarzania i celów przetwarzania (Załącznik nr 1 – Wykaz zbiorów danych osobowych)
b) Ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunków do celów (Załącznik nr 1 – Wykaz zbiorów danych osobowych),
c) Ocenę ryzyka (Załącznik nr 3 – Procedura analizy ryzyka),
d) Środki planowane w celu zaradzenia ryzyku, przedstawione w postaci planu postępowania z ryzykiem (Załącznik nr 3 – Procedura analizy ryzyka).

§12

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) 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 WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
małe (do 10000 PLN, incydent prasowy lokalny)	1
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

3.1 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 POZIOM RYZYKA	**WARTOŚĆ [R = P*S]**
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

3.2 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
3. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka
4. Analizę ryzyka przeprowadza się w specjalnym szablonie, która stanowi załącznik nr 3 do niniejszej Polityki.

3.3 Ponowna analiza ryzyka

1. Ponowna analiza ryzyka przeprowadzana jest nie rzadziej niż raz w roku lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne).
2. Bezpośredni nadzór nad procesem zarządzania sprawuje Rektor przy pomocy IOD.
3. Monitorowanie zmiany poszczególnych elementów ryzyka, w szczególności zagrożeń dokonuje Kierownik Działu Informatyki.

Rozdział 4

Postępowanie na wypadek zagrożenia bezpieczeństwa danych osobowych. Instrukcja postępowania z incydentami.

§13

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 pracownik uczelni zobowiązany jest niezwłocznie, najpóźniej do 24 h, do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego lub Inspektora Ochrony Danych.
2. Do typowych podatności bezpieczeństwa danych osobowych należą w szczególności:
    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 w szczególności:
    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 (bądź 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 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.
8. W przypadku zaistnienia incydentu Administrator powiadamia osoby, których dane dotyczą o zaistniałym incydencie.

Rozdział 5

Regulamin Ochrony Danych Osobowych, polityka kluczy.

§14

1. Regulamin określa podstawowe obowiązki z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami dla: pracowników, współpracowników, pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora/Podmiot przetwarzający, użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora/Podmiot przetwarzający.
2. Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania (Załącznik nr 6 – Oświadczenie o poufności).
3. Polityka kluczy ma na celu techniczne zapewnienie bezpieczeństwa danych osobowych. Polityka kluczy stanowi załącznik do niniejszej Polityki – Załącznik nr 7.

Rozdział 6

Szkolenia/ audyt

§15

1. Każdy użytkownik przed dopuszczeniem do przetwarzania danych osobowych podlega przeszkoleniu z przepisów w tym zakresie oraz wynikających z nich zadań i obowiązków.
2. Wszyscy użytkownicy podlegają okresowym szkoleniom.
3. Za przeprowadzenie szkolenia odpowiada IOD.
4. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia.
5. Po przeprowadzeniu szkolenia z zasad ochrony danych osobowych, uczestnicy są zobowiązani do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.
6. 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 nr 8 – Procedura audytów).

Rozdział 7

Środki organizacyjne i techniczne zabezpieczające dane osobowe

§16

1. Administrator prowadzi uproszczony wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych (Załącznik nr 9 – Wykaz zabezpieczeń).
2. Administrator opracował dokument – Instrukcja zarządzania systemami informatycznymi – wykaz zabezpieczeń w PWSTE w Jarosławiu.
3. Wykaz powinien być aktualizowany, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka/oceny skutków.

§17

1. 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.
2. Procedury przywracania dostępności danych osobowych i dostępu do nich zostały opracowane, jako załącznik – Załącznik nr 10 – Plan ciągłości działania.

Rozdział 8

Wykaz pomieszczeń wchodzących w skład przetwarzania danych osobowych PWSTE w Jarosławiu

§18

Wykaz pomieszczeń należących do PWSTE w Jarosławiu, w których dokonuje się operacji na danych osobowych, z uwzględnieniem pomieszczeń szczególnie chronionych stanowi załącznik do niniejszej Polityki – Załącznik nr 11 – Wykaz pomieszczeń.