

**Efekty uczenia się dla studiów podyplomowych:
Ochrona danych osobowych i bezpieczeństwo informacji w jednostkach sektora publicznego**

Kod składnika opisu charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy Kwalifikacji lub/i kod składnika opisu efektów uczenia się charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji typowych dla kwalifikacji o charakterze zawodowym – poziomy 1–8	Opis charakterystyk drugiego stopnia efektów uczenia się dla kwalifikacji na poziomach 6-8 Polskiej Ramy Kwalifikacji lub/i opis charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji typowych dla kwalifikacji o charakterze zawodowym – poziomy 1–8	Symbol efektu uczenia się dla studiów podyplomowych	Opis efektów uczenia się dla studiów podyplomowych
1	2	3	4
WIEDZA: absolwent zna i rozumie			
P7S_WG	w pogłębionym stopniu – wybrane fakty, obiekty i zjawiska oraz dotyczące ich metody i teorie wyjaśniające złożone zależności między nimi, stanowiące zaawansowaną wiedzę ogólną z zakresu dyscyplin naukowych lub artystycznych tworzących podstawy teoretyczne, uporządkowaną i podbudowaną teoretycznie wiedzę obejmującą kluczowe zagadnienia oraz wybrane zagadnienia z zakresu zaawansowanej wiedzy szczegółowej – właściwe dla programu studiów, główne tendencje rozwojowe dyscyplin naukowych lub artystycznych, do których jest przyporządkowany kierunek studiów	SP_P7S_WG1	w pogłębionym stopniu zagadnienia z zakresu ochrony danych osobowych i bezpieczeństwa informacji oraz dyscyplin naukowych, właściwych dla sektora jednostek publicznych
		SP_P7S_WG2	w pogłębionym stopniu priorytety służące realizacji określonego zadania w zakresie ochrony danych osobowych i bezpieczeństwa informacji
		SP_P7S_WG3	sposoby przeciwdziałania zagrożeniom w zakresie ochrony danych osobowych
		SP_P7S_WG4	rodzaje powiązań wewnątrz systemowych w polskim systemie prawa oraz powiązania tego systemu z prawem Unii Europejskiej oraz systemem prawa międzynarodowego
		SP_P7S_WG5	jakie miejsce zajmuje człowiek w społeczeństwie, jego obowiązki i prawa oraz zasady ochrony
		SP_P7S_WG6	w sposób pogłębiony zagadnienia ekonomiczne, społeczne i psychologiczne wpływające na bezpieczeństwo

			informacji i ochronę danych
		SP_P7S_WG7	regulacje prawne i rozwiązania administracyjno-organizacyjne dotyczące ochrony danych osobowych i bezpieczeństwa informacji w Unii Europejskiej
P7S_WK	fundamentalne dylematy współczesnej cywilizacji ekonomiczne, prawne, etyczne i inne uwarunkowania różnych rodzajów działalności zawodowej związanej z kierunkiem studiów, w tym zasady ochrony własności przemysłowej i prawa autorskiego, podstawowe zasady tworzenia i rozwoju różnych form przedsiębiorczości	SP_P7S_WK1	uwarunkowania i możliwości rozwoju indywidualnej kreatywności w rozwiązywaniu problemów związanych z ochroną danych osobowych i bezpieczeństwem informacji
		SP_P7S_WK2	zasady zarządzania zasobami własności intelektualnej, kontroli i audytu, zarządzania jakością w instytucjach
		SP_P7S_WK3	zasady tworzenia i rozwoju form indywidualnej przedsiębiorczości
		SP_P7S_WK4	w pogłębiony sposób zjawiska stanowiące realne i potencjalne zagrożenia w sferze bezpieczeństwa informacji
UMIEJĘTNOŚCI: absolwent potrafi			
P7S_UW	wykorzystywać posiadaną wiedzę – formułować i rozwiązywać złożone i nietypowe problemy oraz innowacyjnie wykonywać zadania w nieprzewidywalnych warunkach przez: – właściwy dobór źródeł i informacji z nich pochodzących, dokonywanie oceny, krytycznej analizy, syntezy, twórczej interpretacji i prezentacji tych informacji, – dobór oraz stosowanie właściwych metod i narzędzi w tym zaawansowanych technik informacyjno-komunikacyjnych, – przystosowanie istniejących lub opracowanie nowych metod i narzędzi formułować i testować hipotezy związane z prostymi problemami badawczymi	SP_P7S_UW1	interpretować zjawiska i zagrożenia (społeczne, prawne, ekonomiczne) w skali regionalnej i globalnej związane z ochroną danych osobowych i bezpieczeństwem informacji
		SP_P7S_UW2	oceniać jakość przedsięwzięć zmierzających do poprawy sytuacji związanych z ochroną danych osobowych i bezpieczeństwem informacji w jednostkach sektora publicznego
		SP_P7S_UW3	posługiwać się wybranymi normami i regułami (prawnymi, zawodowymi, etycznymi) w celu rozwiązania konkretnego problemu z zakresu ochrony danych osobowych i bezpieczeństwa informacji
P7S_UK	komunikować się na tematy specjalistyczne ze zróżnicowanymi kręgami odbiorców, prowadzić debatę, posługiwać się językiem obcym na poziomie B2+ Europejskiego Systemu Opisu Kształcenia Językowego oraz specjalistyczną terminologią	SP_P7S_UK1	wypowiadać się klarownie, spójnie i precyzyjnie w mowie i na piśmie na tematy związane z ochroną danych osobowych i bezpieczeństwem informacji, wykorzystując zaawansowane teorie oraz źródła
P7S_UO	kierować pracą zespołu współdziałać z innymi osobami w ramach prac zespołowych i podejmować wiodącą rolę w zespołach	SP_P7S_UO1	inicjować projekty mające na celu korygowanie nieprawidłowych ludzkich zachowań i postaw
P7S_UU	samodzielnie planować i realizować własne uczenie się przez całe życie i ukierunkowywać innych w tym zakresie	SP_P7S_UU1	w sposób pogłębiony wyznaczać kierunki rozwoju osobistego i samokształcenia w zakresie ochrony danych osobowych i bezpieczeństwa informacji w jednostkach

			sektora publicznego oraz w wymiarze interdyscyplinarnym
		SP_P7S_UU2	w pogłębiony sposób realizować wyznaczony kierunek rozwoju osobistego i samokształcenia w zakresie ochrony danych osobowych i bezpieczeństwa informacji w jednostkach sektora publicznego
		SP_P7S_UU3	ukierunkowywać innych do osobistego rozwoju w zakresie poszukiwania optymalnych rozwiązań problemów z zakresu ochrony danych osobowych i bezpieczeństwa informacji w jednostkach sektora publicznego
KOMPETENCJE SPOŁECZNE: absolwent jest gotów do			
P7S_KR	odpowiedzialnego pełnienia ról zawodowych z uwzględnieniem zmieniających się potrzeb społecznych, w tym: – rozwijania dorobku zawodu, – podtrzymywania etosu zawodu, – przestrzegania i rozwijania zasad etyki zawodowej oraz działania na rzecz przestrzegania tych zasad	SP_P7S_KR1	świadomego znaczenia zachowania się w sposób profesjonalny i etyczny
		SP_P7S_KR2	odpowiedzialnego wykonywania zawodu w poczuciu jego misji
P7S_KK	krytycznej oceny posiadanej wiedzy i odbieranych treści, uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz zasięgania opinii ekspertów w przypadku trudności z samodzielnym rozwiązaniem problemu	SP_P7S_KK1	krytycznej oceny przyswajanych treści specjalistycznych
		SP_P7S_KK2	systematycznego uzupełniania wiedzy, doskonalenia umiejętności zawodowych oraz kreatywnego poszukiwania rozwiązań problemów dostrzeganych w funkcjonowaniu jednostek sektora publicznego
P7S_KO	wypełniania zobowiązań społecznych, inspirowania i organizowania działalności na rzecz środowiska społecznego, inicjowania działania na rzecz interesu publicznego, myślenia i działania w sposób przedsiębiorczy	SP_P7S_KO1	wdrażania projektów i wykonywania zadań w sferze sektora publicznego
		SP_P7S_KO2	aktywizowania różnych grup społecznych, do inicjowania przedsięwzięć na rzecz ochrony danych osobowych i bezpieczeństwa informacji w jednostkach sektora publicznego

Po ukończeniu studiów podyplomowych absolwent uzyskuje kwalifikacje cząstkowe na poziomie 7 Polskiej Ramy Kwalifikacji.

Objaśnienia:

Kolumna nr 1 i 2 – na podstawie Rozporządzenia MNiSW z dnia 14 listopada 2018 r. (Dz. U. z 2018 roku, poz. 2218) oraz Rozporządzenia MEN z dnia 13 kwietnia 2016 r. w sprawie charakterystyk drugiego stopnia Polskiej Ramy Kwalifikacji typowych dla kwalifikacji o charakterze zawodowym – poziomy 1–8 (Dz. U. z 2016 roku, poz. 537)

Kolumna nr 3 – symbol efektu uczenia się dla studiów podyplomowych

W – kategoria wiedza/ G – głębia; / K – kontekst

U – kategoria umiejętności/ W – wykorzystanie wiedzy; / K – komunikowanie się; / O – organizacja; / U – uczenie się

K – kategoria kompetencje społeczne / K – ocena krytyczna; /O – odpowiedzialność; /R – rola zawodowa

1, 2, 3 i kolejne – numer efektu uczenia się

Kolumna nr 4 – opis treści efektów uczenia się

TREŚCI KSZTAŁCENIA

Nazwa studiów podyplomowych: „**Ochrona danych osobowych i bezpieczeństwo informacji w jednostkach sektora publicznego**”

Wymiar kształcenia (sem.): dwa semestry

CHARAKTERYSTYKA TREŚCI KSZTAŁCENIA

1. Nazwa przedmiotu: **Międzynarodowe, europejskie podstawy ochrony danych osobowych**

Cel kształcenia i treści merytoryczne:

poznanie genezy prawnej ochrony danych osobowych w prawie międzynarodowym i europejskim oraz obecnych regulacji prawnych dotyczących ochrony danych osobowych w prawie międzynarodowym i europejskim.

Efekty uczenia się:

wiedza: posiada wiedzę z zakresu regulacji prawnych obowiązujących w Unii Europejskiej oraz prawie międzynarodowym;

umiejętności: posiada umiejętność formułowania i rozwiązywania problemów z zakresu danych osobowych lub bezpieczeństwa informacji w oparciu o regulacje prawne poza krajowe, posiada umiejętność przekazywania praktycznych konsekwencji wynikających z obowiązujących regulacji europejskich i międzynarodowych, ukierunkowuje innych do samodzielnego poszukiwania optymalnych rozwiązań w prawie międzynarodowym i unijnym powstających problemów w zakresie ochrony danych osobowych, potrafi klarownie i spójnie się wypowiadać w kwestii ochrony danych osobowych na gruncie prawa europejskiego i międzynarodowego;

kompetencje społeczne: potrafi brać odpowiedzialność za powierzone mu zadania, umie wykorzystać wiedzę w rozwiązywaniu problemów praktycznych, myśli i działa krytycznie oraz w sposób przedsiębiorczy, przestrzega zasad etyki zawodowej.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG4; SP_P7S_WG7; SP_P7S_UW1; SP_P7S_UW3; SP_P7S_UK1; SP_P7S_UU1; SP_P7S_UU3; SP_P7S_KK1; SP_P7S_KK2; SP_P7S_KR1; SP_P7S_KR2;

Liczba ECTS: 1,0

2. Nazwa przedmiotu: **Krajowe podstawy ochrony danych osobowych (Konstytucja, ustawa o ochronie danych osobowych, KRI i jego praktyczne znaczenie, zasady przetwarzania danych osobowych)**

Cel kształcenia i treści merytoryczne:

poznanie Konstytucyjnych podstaw ochrony danych osobowych, obowiązującej i poprzedniej ustawy o ochronie danych osobowych, Krajowym Ram Interoperacyjności w zakresie wymaganym dla jednostek sektora publicznego, szczegółowe zapoznanie się podstawami legalizującymi przetwarzanie danych osobowych).

Efekty uczenia się:

wiedza: posiada rozszerzoną wiedzę z zakresu prawnych regulacji obowiązujących w Polsce dotyczących danych osobowych i bezpieczeństwa informacji oraz ich relacji do uregulowań Unijnych, posiada wiedzę z zakresu praktycznego zdiagnozowania problemu w zakresie ochrony danych i wskazania jego prawnego rozwiązania;

umiejętności: posiada umiejętność formułowania i rozwiązywania problemów z zakresu danych osobowych lub bezpieczeństwa informacji w oparciu o krajowe regulacje prawne, wyznacza kierunki samokształcenia w zakresie ochrony danych osobowych i jej realizuje w ramach osobistego rozwoju, ukierunkowuje innych do pogłębionego rozwoju w zakresie ochrony danych osobowych i bezpieczeństwa informacji w jednostkach sektora publicznego (dalej jako: jsp);

kompetencje społeczne: krytycznie ocenia funkcjonujące w jsp rozwiązania w zakresie ochrony danych osobowych i bezpieczeństwa informacji, kreatywnie rozwiązuje problemy z zakresu ochrony danych osobowych w jsp.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG1; SP_P7S_WG4; SP_P7S_WK1; SP_P7S_UW3; SP_P7S_UU1; SP_P7S_UU2; SP_P7S_KK1; SP_P7S_KK2;

Liczba ECTS: 1,5

3. Nazwa przedmiotu: **Etyka zawodowa**

Cel kształcenia i treści merytoryczne:

poznanie zasad deontologicznych jakimi winien kierować się zarówno administrator danych osobowych jak i inspektor ochrony danych osobowych. Uzmysłowanie jak ważne są zasady etyki w codziennej praktyce osób przetwarzających dane osobowe.

Efekty uczenia się:

wiedza: posiada wiedzę z zakresu prawa i obowiązków każdego człowieka w zakresie ochrony danych osobowych i ich etycznych konsekwencji, posiada wiedzę w zakresie psychologicznych aspektów ochrony bezpieczeństwa informacji, posiada umiejętność wskazania etycznych aspektów ochrony danych osobowych i bezpieczeństwa informacji oraz dąży do rozwoju indywidualnej kreatywności w tym zakresie;

umiejętności: kieruje pracą zespołu oraz współdziała z innymi osobami w zakresie korygowania nieprawidłowych postaw etycznych mających wpływ na ochronę danych osobowych i bezpieczeństwa informacji w jsp, wyznacza kierunki i realizuje wyznaczony kierunek rozwoju własnego w zakresie kształtowania postaw etycznych zwiększających bezpieczeństwo danych osobowych i informacji będących w zasobach jsp;

kompetencje społeczne: odpowiedzialnie pełni rolę inspektora ochrony danych osobowych, ma świadomość znaczenia zachowania się w sposób etyczny i profesjonalny, przestrzega i rozwija zasady etyki zawodowej.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG5; SP_P7S_WG6; SP_P7S_WK1; SP_P7S_UO1; SP_P7S_UU1; SP_P7S_KR1; SP_P7S_KR2;

Liczba ECTS: 1,0

4. Nazwa przedmiotu: **System ochrony danych osobowy i bezpieczeństwa informacji (europejskie i krajowe organy nadzoru, zakres kompetencji, uprawnień, kontrole NIK w zakresie ochrony danych i bezpieczeństwa informacji)**

Cel kształcenia i treści merytoryczne:

poznanie systemu (kompetencji, zasad, działania, kontroli organów do tego powołanych) ochrony danych osobowych i bezpieczeństwa informacji, zarówno krajowego jak i europejskiego, poznanie uprawnień jakie w tym zakresie ma Najwyższa Izba Kontroli.

Efekty uczenia się:

wiedza: posiada pogłębioną wiedzę w zakresie systemu ochrony danych osobowych, zna i potrafi wskazać kompetencje poszczególnych organów powołanych do kontroli danych osobowych i bezpieczeństwa informacji, zna zasady przeprowadzania audytu, posiada praktyczną wiedzę o realnych i potencjalnych zagrożeniach wynikających z bezpieczeństwa danych osobowych i informacji;

umiejętności: w pogłębiony sposób wyznacza i realizuje kierunki rozwoju osobistego w zakresie kompetencji, uprawnień i zadań działania organów kontrolnych, potrafi interpretować zagrożenie związane z ochroną danych osobowych i bezpieczeństwa informacji;

kompetencje społeczne: kreatywnie poszukuje możliwości rozwiązania problemów wskazanych podczas kontroli jsp przez organy kontrolne, wdraża projekty minimalizujące zagrożenia związane z ochroną danych osobowych i bezpieczeństwa informacji w jsp.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG1; SP_P7S_WG3; SP_P7S_WK2; SP_P7S_WK4; SP_P7S_UW1; SP_P7S_UU1; SP_P7S_UU2; SP_P7S_KK2; SP_P7S_KO1;

Liczba ECTS: 1,5

5. Nazwa przedmiotu: **Dokumentacja dotycząca ochrony danych osobowych i bezpieczeństwa informacji w jednostce sektora publicznego na podstawie RODO, prawne i praktyczne zasady jej tworzenia**

Cel kształcenia i treści merytoryczne:

poznanie zasad tworzenia, elementów obligatoryjnych i fakultatywnych dokumentacji dotyczącej ochrony danych osobowych jaka powinna być na podstawie RODO w każdej jednostce sektora publicznego.

Efekty uczenia się:

wiedza: posiada rozszerzoną wiedzę dotyczącą potrzebnej w każdej jednostce publicznej dokumentacji dotyczącej ochrony danych osobowych, zasad jej tworzenia i weryfikacji, posiada realną wiedzę o zagrożeniach i potencjalnych zagrożeniach bezpieczeństwa informacji, którą wykorzystuje do przygotowania niezbędnej dokumentacji w tym zakresie w jsp;

umiejętności: inicjuje działania zmierzające do zweryfikowania poprawności przygotowanej dokumentacji w zakresie ochrony danych osobowych i bezpieczeństwa informacji w jsp, wyznacza kierunki rozwoju osobistego i podejmuje samokształcenie w zakresie niezbędnym do zweryfikowania poprawności funkcjonujących rozwiązań w zakresie bezpieczeństwa publicznego w jsp;

kompetencje społeczne: ma świadomość i znaczenie roli jaka dokumentacja pełni w jsp, systematycznie uzupełnia wiedzę w zakresie niezbędnym do oceny poprawności przyjętej dokumentacji, poszukuje rozwiązań zmierzających do poprawy przyjętej w jsp dokumentacji celem zwiększenia bezpieczeństwa danych i informacji, aktywizuje kadrę zarządzającą oraz pozostałych pracowników jsp do podejmowania działań zwiększających bezpieczeństwo danych i posiadanych informacji.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG1; SP_P7S_WG3; SP_P7S_WK4; SP_P7S_UW2; SP_P7S_UO1; SP_P7S_UU2; SP_P7S_KK2; SP_P7S_KO2;

Liczba ECTS: 1,5

6. Nazwa przedmiotu: **Analiza ryzyka i jej znaczenie w zakresie bezpieczeństwa informacji jako podstawowy element procesu zarządzania bezpieczeństwem danych oraz ocena skutków dla ochrony danych osobowych**

Cel kształcenia i treści merytoryczne:

zrozumienie jak ważna jest analiza ryzyka dla wszystkich procesów związanych z zabezpieczeniem przetwarzania danych osobowych, poznanie zasad przeprowadzania analizy ryzyka, poznanie zasad przeprowadzania oceny skutków dla ochrony danych osobowych i ich praktycznego znaczenia.

Efekty uczenia się:

wiedza: posiada wiedzę w zakresie zasad sporządzania analizy ryzyka i zna jej znaczenie przy projektowaniu rozwiązań w zakresie bezpieczeństwa danych osobowych i informacji, posiada

niezbędną wiedzę w zakresie zarządzania ryzykiem, posiada wiedzę o realnych i potencjalnych zagrożeniach jakie mogą wystąpić w jsp, które winny być uwzględnione przy analizie ryzyka;

umiejętności: posiada umiejętność przekazywania wiedzy na temat ryzyka i jego konsekwencji dla bezpieczeństwa informacji i danych osobowych, inicjuje i współdziała przy realizacji projektów i zadań mających na celu zrozumienie problematyki ryzyka w jsp i jego praktycznych aspektów;

kompetencje społeczne: ma świadomość znaczenia analizy ryzyka przy wszystkich czynnościach związanych z bezpieczeństwem informacji i danych osobowych oraz etycznych i profesjonalnych zachowań w tym zakresie, systematycznie uzupełnia wiedzę, doskonali umiejętności w zakresie wykorzystania ryzyka do zwiększenia bezpieczeństwa procesów zachodzących w jsp związanych z bezpieczeństwem informacji oraz danych osobowych.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG3; SP_P7S_WK2; SP_P7S_WK4; SP_P7S_UK1; SP_P7S_UO1; SP_P7S_KR1; SP_P7S_KK2;

Liczba ECTS: 1,5

7. Nazwa przedmiotu: **Klauzula informacyjna w poszczególnych jednostkach i procedurach - obowiązki organów administracji publicznej w związku z koniecznością podania informacji o jakich mowa w art. 13 ust. 1 i 2 RODO na gruncie k.p.a., ordynacji podatkowej, postępowania egzekucyjnego, placówkach edukacyjnych, służbie zdrowia**

Cel kształcenia i treści merytoryczne:

poznanie zasad tworzenia i podawania ogólnej klauzuli informacyjnej na podstawie RODO, poznanie specyfiki tej klauzuli na gruncie k.p.a., ordynacji podatkowej, w placówkach edukacyjnych i służby zdrowia. Rozumień znaczenia tej klauzuli, konieczności jej podawania, przedstawienie szczegółowe i omówienie każdego z elementów obligatoryjnych klauzuli.

Efekty uczenia się:

wiedza: posiada wiedzę z zakresu konieczności i zasad wykonywania ogólnej klauzuli informacyjnej oraz zna priorytety służące realizacji zadań w zakresie danych osobowych, znaczeniu jej dla praw obywatela, obowiązków administratora danych

umiejętności: w pogłębiony sposób realizuje wyznaczone sobie kierunki rozwoju osobistego w zakresie poszerzania wiedzy o sposobach i prawnych obowiązkach w zakresie wykonywania ogólnej klauzuli informacyjnej, potrafi ocenić przedsięwzięcia związane z ochroną danych osobowych oraz rozwiązać konkretne problemy z tego zakresu

kompetencje społeczne: krytycznie ocenia analizowane klauzule informacyjne, potrafi przygotować i wdrożyć ogólną klauzulę informacyjną w danych jsp.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG2; SP_P7S_WG5; SP_P7S_UW2; SP-P7S-UW3; SP_P7S_UU2; SP_P7S_KK1;; SP_P7S_KO1;

Liczba ECTS: 1,0

8. Nazwa przedmiotu: **Warsztaty: szyfrowanie danych osobowych na przenośnych nośnikach, dyskach, mailach**

Cel kształcenia i treści merytoryczne:

poznanie zasad minimalizacji zagrożenia poprzez pesudonimizację. Nabycie praktycznych umiejętności w zakresie szyfrowania nośników danych oraz komunikacji mailowej.

Efekty uczenia się:

wiedza: posiada praktyczną i pogłębioną wiedzę z zakresu znaczenia szyfrowania danych i nośników informacji w praktyce jsp, rozumie prawne, ekonomiczne i etyczne znaczenie szyfrowania danych i nośników informacji, rozumie realne i potencjalne zagrożenia wynikające z braku szyfrowania danych i nośników informacji;

umiejętności: potrafi szyfrować dane i nośnik informacji, potrafi posiadane umiejętności przekazać innym osobom, wskazać im jak poszukiwać optymalnych rozwiązań w tym zakresie;

kompetencje społeczne: odpowiedzialnego wykonywania swoich zadań w poczuciu swojej misji, wdrażania zadań związanych z szyfrowaniem danych i nośników w jsp.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG1; SP_P7S_WG6; SP_P7S_WK2; SP_P7S_WK4; SP_P7S_UO1; SP_P7S_UU3; SP_P7S_KR2; SP_P7S_KO1;

Liczba ECTS: 1,0

9. Nazwa przedmiotu: **Dostęp do informacji publicznej i informacji i ponowne wykorzystanie informacji sektora publicznego, a ochrona danych osobowych**

Cel kształcenia i treści merytoryczne:

poznanie zasad, reguł dostępu do informacji publicznej oraz wyjątków pozwalających na nieudostępniania informacji publicznej ze szczególnym uwzględnieniem problematyki danych osobowych. Zasady pisania pism procesowych, elementy obligatoryjne decyzji omawiającej udostępnienia żądanej informacji. Zapoznanie się z zasadami ponownego wykorzystania informacji sektora publicznego – zasady sporządzania oferty, weryfikacja wymogów formalnych, możliwe rozstrzygnięcia.

Efekty uczenia się:

wiedza: zna zasady udostępniania informacji publicznej oraz ponownego wykorzystania informacji sektora publicznego, rozumie zadania jsp w zakresie udostępniania informacji publicznej i konsekwencji ich niespełniania, zna zasady rozwiązywania problemów pojawiających się przy udostępnianiu informacji publicznej w Polsce i Unii Europejskiej;

umiejętności: potrafi ukierunkować innych pracowników jsp zobligowanych do udostępniania informacji publicznej do osobistego rozwoju w zakresie poszukiwania optymalnych rozwiązań problemów wynikających z obowiązków nałożonych na jsp w zakresie udostępniania informacji publicznej oraz potrafi stosować przepisy w celu prawidłowego udostępniania informacji;

kompetencje społeczne: na świadomość znaczenia zachowania się w sposób profesjonalny przy rozpatrywaniu wniosków o dostęp do informacji publicznej, systematycznie uzupełnia wiedzę w zakresie nowych obowiązków wynikających z udostępniania informacji publicznej.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG1; SP_P7S_WG3; SP_P7S_WK1; SP_P7S_UW1; SP-P7S-UW3; SP_P7S_UU3; SP_P7S_KR1; SP_P7S_KK2;

Liczba ECTS: 1,0

10. Nazwa przedmiotu: **Główne problemy dotyczące ochrony danych osobowych na gruncie:**

- **prawa karnego (przepisy karne, kradzież tożsamości, wyludzanie danych, cyberbezpieczeństwo)**
- **prawa pracy i ubezpieczeń społecznych (zakres danych pozyskiwanych w procesie rekrutacji)**
- **prawa administracyjnego**
- **prawa cywilnego (ochrona dóbr osobistych m.in. wizerunku)**

Cel kształcenia i treści merytoryczne:

poznanie zasad odpowiedzialności za naruszenie zasad przetwarzania danych osobowych w poszczególnych gałęziach prawa i zwrócenie uwagi na specyfikę przetwarzania danych osobowych w prawie pracy (proces rekrutacji, dokumentacja pracownicza, regulaminy socjalne), prawie administracyjnym (przetwarzanie danych wrażliwych przez organ administracji publicznej), prawie cywilnym (ochrona wizerunku, umowy o powierzenie przetwarzania danych).

Efekty uczenia się:

wiedza: zna specyfikę odpowiedzialności za brak przestrzegania zasad ochrony danych osobowych i bezpieczeństwa informacji na gruncie prawa karnego, pracy, administracyjnego i cywilnego, rozumie zasady odpowiedzialności na gruncie prawa krajowego i europejskiego;

umiejętności: potrafi spójnie i klarownie przedstawić praktyczne aspekty ochrony danych osobowych w poszczególnych dziedzinach prawa, wskazując źródła ich ochrony, wyznacza i realizuje kierunki samodoskonalenia w zakresie konsekwencji naruszenia zasad ochrony danych osobowych i bezpieczeństwa informacji w poszczególnych dziedzinach prawa oraz oceniać zasadność stosowanych mechanizmów;

kompetencje społeczne: krytycznej oceny posiadanej wiedzy i odbieranych treści w zakresie konsekwencji związanych z odpowiedzialnością za naruszenie zasad ochrony danych osobowych, aktywizuje pracowników jsp do poszerzenia swej wiedzy w zakresie odpowiedzialności za nieprzestrzeganie zasad dotyczących ochrony danych osobowych i bezpieczeństwa informacji w danej jednostce jsp.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG1; SP_P7S_WG4; SP-P7S-UW2; SP_P7S_UK1; SP_P7S_UU1; SP_P7S_KK1; SP_P7S_KO2;

Liczba ECTS: 2,0

11. Nazwa przedmiotu: **Ochrona danych osobowych w świetle orzecznictwa TSUE i ETPCz – analiza przypadku**

Cel kształcenia i treści merytoryczne:

poznanie najważniejszych z punktu codziennej praktyki orzeczeń TSUE i ETPCz. Poznanie znaczenia i konsekwencji wydanych rozstrzygnięć.

Efekty uczenia się:

wiedza: zna i rozumie relacje pomiędzy europejskim i krajowym system prawnym, oraz konsekwencje praktyczne orzeczeń TSUE i ETPCz, pogłębia wiedzę o prawach człowieka związanych z danymi osobowymi, zna możliwości wykorzystania orzeczeń TSUE i ETPCz do kreatywnego rozwiązywania problemów w zakresie ochrony danych osobowych;

umiejętności: potrafi inicjować projekty mające na celu korygowanie nieprawidłowych postaw w zakresie ochrony danych osobowych przy wykorzystaniu orzecznictwa TSUE i ETPCz;

kompetencje społeczne: ma świadomość znaczenia zachowania się w sposób profesjonalny i etyczny, odpowiedzialnie wykonuje zawód w poczuciu jego misji, rozwija swój dorobek zawodowy.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG4; SP_P7S_WG5; SP_P7S_WK1; SP_UO1; SP_P7S_KR1; SP_P7S_KR2; SP_P7S_KK2;

Liczba ECTS: 1,0

12. Nazwa przedmiotu: **Polityka ochrony danych osobowych – zakres, zasady tworzenia**

Cel kształcenia i treści merytoryczne:

poznanie zasad tworzenia obligatoryjnego w jsp dokumentu jaki jest Polityka Ochrony Danych Osobowych, jego elementów obligatoryjnych i fakultatywnych, zasad weryfikacji, tego dokumentu i jego znaczenia dla jsp.

Efekty uczenia się:

wiedza: zna i rozumie zasady tworzenia polityki ochrony danych osobowych jak elementu przeciwdziałania zagrożeniom wynikającym z ochrony danych osobowych i bezpieczeństwa informacji, rozwiązuje kreatywnie problemy wynikające z tworzenia i wdrożenia polityki bezpieczeństwa ochrony danych osobowych w jsp;

umiejętności: potrafi wyznaczyć kierunki i wdrożyć samokształcenie w zakresie zmieniających się obowiązków związanych z ochroną danych osobowych i bezpieczeństwem informacji, ukierunkowuje innych do osobistego rozwoju w zakresie poszukiwania optymalnych rozwiązań

zmierzających do zoptymalizowania polityki bezpieczeństwa w jsp, potrafi tworzyć politykę ochrony danych osobowych z uwzględnieniem zagrożenia w skali regionalnej i globalnej;

kompetencje społeczne: odpowiedzialnego wykonywania zawodu w poczuciu jego misji, wdrożenia polityki ochrony danych osobowych w jsp.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG3; SP_P7S_WK1; SP_P7S_UW1; SP_P7S_UU1; SP_P7S_UU3; SP_P7S_KR2; SP_P7S_KO1;

Liczba ECTS: 1,5

13. Nazwa przedmiotu: **Monitoring wizyjny w sektorze publicznym i prywatnym**

Cel kształcenia i treści merytoryczne:

poznanie prawnych podstaw tworzenia systemu monitoringu wizyjnego w sektorze publicznym i prywatnym. Omówienie aktualnych problemów prawnych z tym związanych.

Efekty uczenia się:

wiedza: zna zasady tworzenia prawnych regulacji w zakresie monitoringu wizyjnego, posiada pogłębioną wiedzę o realnych i potencjalnych zagrożeniach wynikających z braku regulacji w zakresie monitoringu wizyjnego, zna znaczenie monitoringu wizyjnego w indywidualnej przedsiębiorczości;

umiejętności: inicjuje działania mające na celu zweryfikowanie poprawności regulacji w zakresie monitoringu wizyjnego w jsp;

kompetencje społeczne: systematycznie uzupełnia wiedzę, doskonali umiejętności związane z monitoringiem wizyjnym i zasadami jego wykorzystania, aktywizuje różne grupy społeczne w zakresie zwiększenia świadomości dotyczących prawnego uregulowania monitoringu.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG2; SP_P7S_WK3; SP_P7S_WK4; SP_P7S_UW1; SP_P7S_KK2; SP_P7S_KO2;

Liczba ECTS: 1,0

14. Nazwa przedmiotu: **Prawa dysponentów danych osobowych**

Cel kształcenia i treści merytoryczne:

szczegółowe przedstawienie praw każdego obywatela wynikających z przyjętych regulacji prawnych w obszarze danych osobowych, m.in.: prawo do bycia poinformowanym o operacjach przetwarzania, prawo dostępu do danych i uzyskania ich kopii, prawo do sprostowania/uzupełnienia danych, prawo do usunięcia danych (prawo do bycia zapomnianym), prawo do ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do sprzeciwu, prawo do tego, by nie podlegać profilowaniu. Zasad realizacji tych praw, wyjątków w ich stosowaniu przyjętych w prawie krajowym.

Efekty uczenia się:

wiedza: zna prawa dysponentów danych osobowych, posiada pogłębioną wiedzę o zasadach ochrony praw dysponentów danych, rozumie i zna regulacje prawne i rozwiązania administracyjno – organizacyjne gwarantujące przestrzeganie praw dysponentów danych oraz komunikować zagrożenia społeczne, prawne i ekonomiczne;

umiejętności: klarownie i spójnie potrafi przedstawić prawa dysponentów danych i ich praktyczne znaczenie;

kompetencje społeczne: ma świadomość zaznaczenia zachowania się w sposób profesjonalny i etyczny w stosunku do osób realizujących swoje uprawnienia, aktywizuje różne grupy społeczne do zapoznawania się z przysługującymi im prawami.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG2; SP_P7S_WG7; SP_P7S_UW1; SP_P7S_UK1; SP_P7S_KR1; SP_P7S_KO2;

Liczba ECTS: 1,0

15. Nazwa przedmiotu: **Kontrola i nadzór przestrzegania przepisów o ochronie danych osobowych i bezpieczeństwa informacji**

Cel kształcenia i treści merytoryczne:

poznanie szczegółowych zasad prowadzenia kontroli przestrzegania zasad ochrony danych osobowych przez powołane do tego organy, uprawnień kontrolnych organów, ich kontrolerów, zasad kwestionowania poczynionych ustaleń.

Efekty uczenia się:

wiedza: zna krajowy i europejski system kontroli i nadzoru nad przestrzeganiem przepisów o ochronie danych osobowych i bezpieczeństwa informacji;

umiejętności: inicjuje działania zmierzające do efektywniejszego działania systemu nadzoru i kontroli w zakresie przestrzegania przepisów o ochronie danych osobowych;

kompetencje społeczne: systematycznie uzupełnia wiedzę, kreatywnie poszukuje rozwiązań problemów związanych z funkcjonowaniem systemu nadzoru i kontroli nad przestrzeganiem ochrony danych osobowych, inicjuje działania zwiększające nadzór nad danymi osobowymi w jsp.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG4; SP_P7S_WK2; SP_P7S_UO1; SP_P7S_KK2; SP_P7S_KO1;

Liczba ECTS: 1,0

16. Nazwa przedmiotu: **Administrator danych osobowych, inspektor danych osobowych - pozycja prawna, zakres odpowiedzialności**

Cel kształcenia i treści merytoryczne:

poznanie szczegółowych zadań, obowiązków i uprawnień publicznych administratorów danych, oraz inspektorów ochrony danych osobowych, w tym ich odpowiedzialności za niewłaściwe wykonywanie powierzonych im obowiązków.

Efekty uczenia się:

wiedza: zna zadania i obowiązki administratora danych osobowych i inspektora ochrony danych osobowych, zna sposoby przeciwdziałania zagrożeniom w zakresie ochrony danych osobowych jakie są do dyspozycji administratora danych i inspektora ochrony danych osobowych, zna regulacje prawne europejskie dotyczące administratora danych i inspektora ochrony danych osobowych;

umiejętności: potrafi precyzyjnie, wykorzystując dostępne źródła przedstawić rolę i pozycję administratora danych osobowych i inspektora ochrony danych osobowych w systemie ochrony danych osobowych i bezpieczeństwa informacji, inicjuje działania mające na celu korygowania niepoprawnych zachowań i postaw w zakresie przestrzegania danych osobowych i bezpieczeństwa informacji przez administratora danych i inspektora ochrony danych osobowych;

kompetencje społeczne: krytyczna ocena postawy administratora danych i inspektora ochrony danych osobowych, systematyczne uzupełnianie wiedzy doskonalenie umiejętności zawodowych inspektora ochrony danych osobowych, kreatywne rozstrzyganie problemów jakie ma administrator danych osobowych i inspektor ochrony danych osobowych w jsp.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG2; SP_P7S_WG3; SP_P7S_WG7; SP_P7S_UW1; SP_P7S_UW3; SP_P7S_UK1; SP_P7S_UO1; SP_P7S_KR1; SP_P7S_KK2;

Liczba ECTS: 1,0

17. Nazwa przedmiotu: **Ochrona danych osobowych i bezpieczeństwa informacji – case study**

Cel kształcenia i treści merytoryczne:

poznanie praktycznych aspektów omówionych regulacji prawnych na wybranych przypadkach, wykazanie błędów w działaniu jsp, administratorów tych jednostek, przedstawienie przebiegu

sposobu rozwiązania problemu, konsekwencji bierności czy nieprofesjonalnego zajmowania się problematyką ochrony danych osobowych i bezpieczeństwa informacji.

Efekty uczenia się:

wiedza: prezentuje rozszerzoną wiedzę z zakresu ochrony danych osobowych, która pozwala na rozwiązywanie praktycznych problemów, posiada realną i potencjalną wiedzę o zagrożeniach w sferze bezpieczeństwa informacji, którą można wykorzystać do rozwiązania konkretnych problemów;

umiejętności: inicjować działania mające na celu korygowanie nieprawidłowości w zakresie ochrony danych osobowych i bezpieczeństwa informacji, potrafi rozwiązywać praktyczne problemy związane z ochroną danych osobowych i bezpieczeństwem informacji, przedstawiając klarownie ich źródło i sposób rozwiązania;

kompetencje społeczne: systematycznie uzupełniać wiedzę pozwalającą na kreatywne rozwiązywanie praktycznych problemów z zakresu ochrony danych osobowych i bezpieczeństwa informacji.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG1; SP_P7S_WK1; SP_P7S_WK4; SP_P7S_UW2; SP_P7S_UO1; SP_P7S_UK1; SP_P7S_KK2; SP_P7S_KO1;

Liczba ECTS: 1,0

18. Nazwa przedmiotu: **Bezpieczeństwo informacji w praktyce jednostek sektora publicznego:**

- **informacja, a informacja prawnie chroniona, System zarządzania bezpieczeństwem informacji (dalej jako: SZBI) i co się na niego składa,**
- **opis dokumentacji (rodzaje procedur, dobre praktyki, ciekawe wpadki),**
- **analiza ryzyka, ISO 27001 – omówienie wymagań, Certyfikacja ISO 27001 i certyfikacja RODOwska**

Cel kształcenia i treści merytoryczne:

poznanie systemu bezpieczeństwa i informacji w jsp oraz zasad nim zarządzania, poznanie podstaw norm z grupy ISO 27001, procesów certyfikacji. Wskazanie różnic między ochroną danych osobowych i ochroną bezpieczeństwa informacji.

Efekty uczenia się:

wiedza: zna system zarządzania bezpieczeństwem informacji w jsp, rozumie jego zasady i szuka możliwości jego ulepszenia, zna realne i potencjalne zagrożenia wpływające na bezpieczeństwo informacji w jsp;

umiejętności: potrafi przedstawić zasady tworzenia i funkcjonowania SZBI oraz ocenić jego skuteczność;

kompetencje społeczne: krytycznie ocenić funkcjonujący SZBI pod kątem jego ulepszenia, wdrożyć SZBI w jsp, aktywizując różne grupy społeczne do podejmowania działań na rzecz wzmocnienia SZBI w jsp.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG1; SP_P7S_WG3; SP_P7S_WK4; SP_P7S_UW2; SP_P7S_UK1; SP_P7S_KK1; SP_P7S_KO2;

Liczba ECTS: 1,5

19. Nazwa przedmiotu: **Egzamin**

Cel kształcenia i treści merytoryczne:

zweryfikowanie pozyskanej wiedzy, umiejętności i kompetencji.

Efekty uczenia się:

wiedza: zweryfikowanie wiedzy zakresu ochrony danych osobowych i bezpieczeństwa informacji w sektorze jednostek publicznych w zakresie poruszanych w toku studiów podyplomowych;

umiejętności: w sposób pogłębiony wypowiada się klarownie, spójnie i precyzyjnie w mowie i na piśmie na tematy związane z ochroną danych osobowych i bezpieczeństwem informacji,

wykorzystując zaawansowane teorie oraz źródła, potrafi posługiwać się normami i regułami w celu rozwiązania konkretnego problemu, interpretować zjawiska i zagrożenia w skali regionalnej i globalnej;

kompetencje społeczne: ma świadomość znaczenia zachowania się w sposób profesjonalny i etyczny, kreatywnie poszukuje rozwiązania problemu w zakresie danych osobowych i bezpieczeństwa informacji, projektuje zadania w jsp zmierzające do stałego podnoszenia bezpieczeństwa danych osobowych i informacji oraz minimalizowania zagrożeń.

Symbole efektów uczenia się dla studiów podyplomowych: SP_P7S_WG1; SP_P7S_WG2; SP_P7S_WG3; SP_P7S_WG4; SP_P7S_WG5; SP_P7S_WG6; SP_P7S_WG7; SP_P7S_WK1; SP_P7S_WK2; SP_P7S_WK3; SP_P7S_WK4; SP_P7S_UW1; SP_P7S_UW3; SP_P7S_UK1; SP_P7S_KR1; SP_P7S_KK2; SP_P7S_KO1;

Liczba ECTS: 8,0

PLAN STUDIÓW PODYPLOMOWYCH

Nazwa studiów podyplomowych: „**Ochrona danych osobowych i bezpieczeństwo informacji w jednostkach sektora publicznego**”

Wymiar kształcenia (sem.): dwa semestry

Liczba punktów ECTS konieczna do uzyskania kwalifikacji podyplomowych: 30

Lp.	Nazwa przedmiotu	Rodzaj i wymiar zajęć dydaktycznych				Forma zaliczenia przedmiotu/sposób weryfikacji efektów uczenia się	Punkty ECTS
		Wykłady (godz.)	Ćwiczenia (godz.)	Zajęcia teoretyczne (godz.)	Zajęcia praktyczne (godz.)		
Semestr I							
1	Międzynarodowe, europejskie podstawy ochrony danych osobowych	6	-	6	-	Zaliczenie	1,0
2	Krajowe podstawy ochrony danych osobowych	10	10	10	10	Zaliczenie	1,5
3	Etyka zawodowa	4	-	4	-	Zaliczenie	1,0
4	System ochrony danych osobowy i bezpieczeństwa informacji	10	-	10	-	Zaliczenie	1,5
5	Dokumentacja dotycząca ochrony danych osobowych i bezpieczeństwa informacji w jednostce sektora publicznego na podstawie RODO, prawne i praktyczne zasady jej tworzenia	10	10	10	10	Zaliczenie z oceną	1,5
6	Analiza ryzyka i jej znaczenie w zakresie bezpieczeństwa informacji jako podstawowy element procesu zarządzania bezpieczeństwem danych oraz ocena skutków dla ochrony danych osobowych	-	8	-	8	Zaliczenie z oceną	1,5
7	Klauzula informacyjna w poszczególnych jednostkach i procedurach	-	8	-	8	Zaliczenie	1,0
8	Warsztaty: szyfrowanie danych osobowych na przenośnych nośnikach, dyskach, mailach	-	8	-	8	Zaliczenie z oceną	1,0
Semestr II							
9	Dostęp do informacji publicznej i informacji i ponowne wykorzystanie informacji sektora publicznego, a ochrona danych osobowych	10	-	10	-	Zaliczenie z oceną	1,0
10	Główne problemy dotyczące ochrony danych osobowych na gruncie: prawa karnego, cywilnego, administracyjnego,	24	-	24	-	Zaliczenie	2,0

	prawa pracy i ubezpieczeń społecznych						
11	Ochrona danych osobowych w świetle orzecznictwa TSUE i ETPCz – analiza przypadku	-	6	-	6	Zaliczenie	1,0
12	Polityka ochrony danych osobowych – zakres, zasady tworzenia	10	10	10	10	Zaliczenie z oceną	1,5
13	Monitoring wizyjny w sektorze publicznym i prywatnym	8	0	8	0	Zaliczenie	1,0
14	Prawa dysponentów danych osobowych	10	0	10	0	Zaliczenie z oceną	1,0
15	Kontrola i nadzór przestrzegania przepisów o ochronie danych osobowych i bezpieczeństwa informacji	8	-	8	-	Zaliczenie z oceną	1,0
16	Administrator danych osobowych, inspektor danych osobowych - pozycja prawna, zakres odpowiedzialności	8	-	8	-	Zaliczenie z oceną	1,0
17	Ochrona danych osobowych i bezpieczeństwa informacji – case study	-	10	-	10	Zaliczenie z oceną	1,0
18	Bezpieczeństwo informacji w praktyce jednostek sektora publicznego	10	4	10	4	Zaliczenie	1,5
19	Egzamin	-	-	-	-	Egzamin	8,0
Łączna liczba godzin		128	74	128	74	Łączna liczba punktów ECTS	30
		202		202			

Okres zaliczeniowy na studiach podyplomowych: rok