



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Ochrona danych [N2IBiJ1-JiEwBP>OD]

Przedmiot

Kierunek studiów

Inżynieria bezpieczeństwa i jakości

Rok/Semestr

2/3

Studia w zakresie (specjalność)

Jakość i ergonomia w bezpieczeństwie pracy

Profil studiów

ogólnoakademicki

Poziom studiów

drugiego stopnia

Język oferowanego przedmiotu

polski

Forma studiów

niestacjonarne

Wymagalność

obieralny

Liczba godzin

Wykład

10

Laboratorium

0

Inne

0

Ćwiczenia

10

Projekty/seminaria

0

Liczba punktów ECTS

2,00

Koordynatorzy

dr inż. Marek Goliński

marek.golinski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student posiada podstawową wiedzę, niezbędną do zrozumienia społecznych i prawnych uwarunkowań prowadzenia działalności inżynierskiej. Student posiada umiejętność wykorzystania wskazanych źródeł oraz interpretacji zjawisk społecznych. Student rozumie konieczność poszerzania swoich kompetencji w ramach nauk społecznych.

Cel przedmiotu

Przekazanie studentom wiedzy w zakresie wymogów stawianych przedsiębiorcom i innym organizacjom w zakresie gromadzenia i przetwarzania danych osobowych oraz zasady odpowiedzialności prawnej stąd wynikającej.

Przedmiotowe efekty uczenia się

Wiedza:

1. Student zna w pogłębionym stopniu tendencje rozwojowe oraz dobre praktyki dotyczące zarządzania bezpieczeństwem w szczególności bezpieczeństwem danych w organizacjach w ujęciu lokalnym i globalnym [K2_W04].
2. Student zna w pogłębionym stopniu zasady przepływu informacji, komunikacji, uwarunkowań

prawnych i regulacyjnych wpływających na ochronę danych charakterystyczne dla obszaru zarządzania bezpieczeństwem organizacji [K2_W14].

Umiejętności:

1. Student potrafi stosować metody i narzędzia rozwiązywania złożonych i nietypowych problemów oraz zaawansowane techniki informacyjno-komunikacyjne charakterystyczne dla środowiska zawodowego związanego z zarządzaniem i ochroną danych w organizacjach [K2_U02].
2. Student potrafi dobrać i zastosować narzędzia komputerowego wspomaganie rozwiązywania problemów charakterystycznych dla zarządzania sferą ochrony danych w organizacjach [K2_U0].

Kompetencje społeczne:

1. Student jest krytyczny wobec swojej wiedzy, jest gotów do zasięgania opinii ekspertów podczas rozwiązywania problemów poznawczych i praktycznych, ciągłego dokształcania z branży IT i regulacji prawnych, w szczególności związanych z ochroną danych w obszarze zarządzania bezpieczeństwem w organizacjach [K2_K01].
2. Student prawidłowo identyfikuje i rozstrzyga dylematy związane z szeroko pojętym bezpieczeństwem, szczególnie w obszarze danych, rozumie konieczność uświadamiania społeczeństwa w zakresie potrzeby kształtowania bezpieczeństwa w różnych obszarach funkcjonowania organizacji [K2_K02].

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykład: ocena formująca dyskusje podsumowujące poszczególne wykłady, rozwiązywane w trakcie zajęć problemy prawne, dające możliwość oceny zrozumienia problematyki przez studenta.

Wiedza nabyta w ramach wykładu jest weryfikowana przez dwa 15-minutowe kolokwia, z których każde składa się z 5- 10 pytań, różnie punktowanych, konieczność zaliczenia obu kolokwiów.

Ćwiczenia: wiedza nabyta w ramach ćwiczeń jest weryfikowana przez dwa 15-minutowe kolokwia, z których każde składa się z 5- 10 pytań, różnie punktowanych, konieczność zaliczenia obu kolokwiów.

Skala ocen:

- 0-50 pkt - 2.0;
- 51-60 pkt - 3.0;
- 61-70 pkt - 3.5;
- 71-80 pkt - 4.0;
- 81-90 pkt - 4.5;
- 91-100 pkt - 5.0

Treści programowe

Wykład:

Pojęcie, geneza i źródła prawa ochrony danych osobowych. Definicja danych osobowych, ich rodzaje i szczególne kategorie. Zasady przetwarzania danych osobowych "wrażliwych" i "zwykłych". Powierzenie przetwarzania danych a udostępnianie danych. Prawa osób, których dane poddawane są przetwarzaniu. Obowiązki administratora i podmiotu przetwarzającego dane. Wyznaczanie, status i zadania inspektora ochrony danych. Zapewnienie zgodności i dokumentacja ochrony danych osobowych. Ocena ryzyka.

Ćwiczenia:

Case study - procesy przetwarzania danych osobowych w firmie. Rodzaje dokumentów związanych z wybranymi procesami przetwarzania danych w firmie. Umowa o dzieło/zlecenie, umowa powierzenia przetwarzania danych osobowych, zgoda na wykorzystanie wizerunku, przetwarzanie danych zwykłych i sensytywnych. Ochrona danych osobowych w miejscu pracy. Ochrona i bezpieczeństwo danych osobowych z punktu widzenia osoby fizycznej i osoby prawnej, z uwzględnieniem wyzwań wynikających z funkcjonowania w świecie cyfrowym.

Tematyka zajęć

Wykład:

Pojęcie, geneza i źródła prawa ochrony danych osobowych

Pojęcie danych osobowych: Definicja danych osobowych, jakie informacje uznawane są za dane osobowe. Geneza prawa ochrony danych osobowych: Historia powstania regulacji dotyczących ochrony danych osobowych, rozwój prawa na przestrzeni lat.

Źródła prawa ochrony danych osobowych: Dokumenty międzynarodowe, unijne i krajowe, które regulują ochronę danych osobowych (np. RODO, ustawa o ochronie danych osobowych).

Definicja danych osobowych, ich rodzaje i szczególne kategorie

Rodzaje danych osobowych: Podział na dane zwykłe i dane szczególne (wrażliwe), różnice między nimi.

Szczególne kategorie danych osobowych: Dane dotyczące zdrowia, pochodzenia rasowego lub etnicznego, przekonań religijnych, orientacji seksualnej, etc.

Zasady przetwarzania danych osobowych "wrażliwych" i "zwykłych"

Zasady ogólne: Zasady zgodności z prawem, rzetelności, przejrzystości, minimalizacji danych, integralności i poufności.

Specjalne zasady przetwarzania danych wrażliwych: Surowsze wymagania dotyczące przetwarzania danych szczególnych kategorii.

Powierzenie przetwarzania danych a udostępnianie danych

Powierzenie przetwarzania danych: Kiedy i w jaki sposób dane mogą być przetwarzane przez zewnętrzne podmioty na zlecenie administratora.

Udostępnianie danych: Warunki, na jakich dane mogą być udostępniane innym podmiotom, różnice między powierzeniem a udostępnianiem.

Prawa osób, których dane poddawane są przetwarzaniu

Prawo dostępu: Prawo do informacji o przetwarzaniu danych.

Prawo do sprostowania, usunięcia i ograniczenia przetwarzania: Warunki korzystania z tych praw.

Prawo do przenoszenia danych: Możliwość przenoszenia danych do innego administratora.

Prawo do sprzeciwu: Możliwość sprzeciwu wobec przetwarzania danych.

Obowiązki administratora i podmiotu przetwarzającego dane

Administrator danych: Obowiązki dotyczące zapewnienia zgodności z przepisami, zabezpieczenia danych, zgłaszania naruszeń.

Podmiot przetwarzający dane: Obowiązki wynikające z umowy powierzenia przetwarzania danych, odpowiedzialność za zgodność z przepisami.

Wyznaczanie, status i zadania inspektora ochrony danych

Wyznaczanie IOD: Kiedy konieczne jest wyznaczenie Inspektora Ochrony Danych.

Status IOD: Niezależność i ochrona przed zwolnieniem.

Zadania IOD: Monitorowanie zgodności z przepisami, doradztwo, prowadzenie szkoleń.

Zapewnienie zgodności i dokumentacja ochrony danych osobowych

Dokumentacja: Wymagane dokumenty i rejestry, np. rejestr czynności przetwarzania.

Zapewnienie zgodności: Procedury audytowe, polityki ochrony danych.

Ocena ryzyka

Ocena skutków dla ochrony danych: Kiedy jest wymagana, jak przeprowadzać analizę ryzyka związanego z przetwarzaniem danych osobowych.

Ćwiczenia:

Ochrona danych osobowych w stosunkach pracy

Zakres dopuszczalnego gromadzenia i przetwarzania danych osobowych pracowników przez pracodawcę w procesie rekrutacyjnym i w okresie zatrudnienia: Jakie dane mogą być zbierane i przetwarzane, w jakich celach i na jakich zasadach.

Obowiązki pracodawcy jako administratora danych

Administrator danych: Obowiązki pracodawcy wynikające z przepisów, zabezpieczenie danych pracowników, informowanie pracowników o przetwarzaniu ich danych.

Kontrola i postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych

Kontrola: Procedury kontroli przetwarzania danych przez pracodawcę.

Postępowanie w przypadku naruszenia: Kroki, które należy podjąć w przypadku naruszenia ochrony danych, zgłaszanie naruszeń.

Sankcje za nieprzestrzeganie przepisów o ochronie danych osobowych

Odpowiedzialność cywilna: Możliwość dochodzenia roszczeń przez osoby, których dane zostały naruszone.
Odpowiedzialność karna: Sankcje karne za naruszenie przepisów.
Administracyjne kary pieniężne: Wysokość i zasady nakładania kar przez organy nadzorcze.
Ochrona i bezpieczeństwo danych osobowych z punktu widzenia osoby fizycznej i osoby prawnej

Osoba fizyczna: Jak osoby fizyczne mogą chronić swoje dane osobowe.
Osoba prawna: Wyzwania dla firm i instytucji w zakresie ochrony danych, procedury zabezpieczania danych w kontekście cyfrowym.

Metody dydaktyczne

Wykład: prezentacja informacyjna, dyskusja z rozwiązywaniem problemów.
Wykład jest realizowany z wykorzystaniem technik kształcenia na odległość w trybie synchronicznym.
Dopuszczalne platformy: eMeeting, Zoom, Microsoft Teams.
Ćwiczenia: dyskusja z wykorzystaniem prezentacji multimedialnej, metoda przypadków, dyskusja.

Literatura

Podstawowa:

1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483 ze zm.).
2. 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).
3. Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2019 r. poz. 1781 t.j.).
4. Ustawa Kodeks pracy z dnia 26 czerwca 1974 r. (Dz. U. z 2020 r. poz. 1320 t.j.).
5. Fajgielski P. (2019), Prawo ochrony danych osobowych. Zarys wykładu, Wydawnictwo Wolters Kluwer, Warszawa.

Uzupełniająca:

1. Ustawa Kodeks cywilny z dnia 23 kwietnia 1964 r. (Dz. U. 2020 r. poz. 1740 t.j.).
2. Ustawa o prawie autorskim i prawach pokrewnych z dnia 4 02 1994 r. (Dz. U. 2021 r. poz. 1062 t.j.).
3. Ustawa o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2020 r. (Dz. U. 2020 r. poz. 344 t.j.).
4. Majchrzak J., Goliński M., Matura W., The concept of the quality and grey system theory application in marketing information quality cognition and assessment, Central European Journal of Operations Research, 2020, Vol. 28, No. 2.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	50	2,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	20	1,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	30	1,00