



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Ochrona danych [N2IBiJ1-BiZK>OD]

Przedmiot

Kierunek studiów

Inżynieria bezpieczeństwa i jakości

Rok/Semestr

1/2

Studia w zakresie (specjalność)

Bezpieczeństwo i zarządzanie kryzysowe

Profil studiów

ogólnoakademicki

Poziom studiów

drugiego stopnia

Język oferowanego przedmiotu

polski

Forma studiów

niestacjonarne

Wymagalność

obieralny

Liczba godzin

Wykład

0

Laboratorium

0

Inne

0

Ćwiczenia

20

Projekty/seminaria

20

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_U08].

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:

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

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.

Ocena podsumowująca: pisemne zaliczenie przedmiotu w formie testu realizowanego na ostatnich zajęciach ćwiczeniowych. Kolokwium składa się z ok. 10 pytań. Próg zaliczeniowy: 51% punktów. Skala ocen jest zgodna z zasadami opisanymi w Regulaminie Studiów.

Treści programowe

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

Ćwiczenia:

Case Study - Procesy przetwarzania danych osobowych w firmie

Analiza procesów przetwarzania danych: Szczegółowe badanie różnych działań związanych z przetwarzaniem danych w firmie, identyfikacja kroków, zaangażowanych działów oraz ogólnego przepływu pracy. Obejmuje to mapowanie, jak dane przepływają przez organizację i wskazywanie kluczowych punktów zbierania, przetwarzania, przechowywania i usuwania danych.

Rodzaje dokumentów związanych z wybranymi procesami przetwarzania danych w firmie

Umowa o pracę/Umowa zlecenie:

Definicja i różnice między umową o pracę a umową zlecenie.

Kluczowe klauzule dotyczące ochrony danych i poufności.

Procedury zapewniające zgodność z przepisami o ochronie danych w ramach umów.

Umowa powierzenia przetwarzania danych osobowych (DPA):

Przegląd tego, co stanowi DPA.

Niezbędne elementy DPA: obowiązki procesora danych i administratora, środki bezpieczeństwa, procedury zgłaszania naruszeń.

Jak sporządzać i wdrażać DPA w ramach struktury firmy.

Zgoda na wykorzystanie wizerunku:

Znaczenie uzyskania zgody na wykorzystanie wizerunku osoby.

Składniki ważnej zgody: cel, zakres, czas trwania i prawa osoby.

Praktyczne kroki zarządzania i dokumentowania zgody.

Przetwarzanie danych zwykłych i sensytywnych:

Różnice między danymi zwykłymi a sensytywnymi (np. informacje zdrowotne, pochodzenie rasowe lub etniczne).

Specyficzne wymagania dotyczące przetwarzania danych sensytywnych, w tym podstawy prawne i dodatkowe zabezpieczenia.

Przykłady działań związanych z przetwarzaniem danych zwykłych oraz najlepsze praktyki w obsłudze danych sensytywnych.

Ochrona danych osobowych w miejscu pracy

Zbieranie i przetwarzanie danych pracowników:

Wytyczne dotyczące danych pracowników, które można zbierać podczas rekrutacji i zatrudnienia.

Podstawa prawna przetwarzania danych pracowników i zapewnienie przejrzystości.

Techniki minimalizacji zbierania danych i zabezpieczania informacji o pracownikach.

Środki bezpieczeństwa danych w miejscu pracy:

Wdrażanie fizycznych i technicznych środków bezpieczeństwa w celu ochrony danych pracowników.

Szkolenie pracowników na temat zasad ochrony danych i protokołów.

Ustalanie polityk kontroli dostępu do danych oraz regularne audyty w celu zapewnienia zgodności.

Ochrona i bezpieczeństwo danych osobowych z punktu widzenia osoby fizycznej i osoby prawnej

Dla osób fizycznych:

Strategie ochrony danych osobowych przez osoby fizyczne: używanie silnych haseł, rozpoznawanie prób phishingowych, zrozumienie ustawień prywatności.

Prawa osób fizycznych wynikające z przepisów o ochronie danych (np. prawo dostępu, prawo do sprostowania, prawo do usunięcia danych).

Kroki, które mogą podjąć osoby fizyczne w przypadku naruszenia prywatności danych, w tym składanie skarg i poszukiwanie środków prawnych.

Dla osób prawnych:

Wyzwania, przed którymi stoją firmy w zakresie ochrony danych osobowych w erze cyfrowej.

Opracowywanie kompleksowych polityk ochrony danych i integracja ich z kulturą organizacyjną.

Stosowanie technik szyfrowania, anonimizacji i pseudonimizacji w celu zwiększenia bezpieczeństwa danych.

Przeprowadzanie regularnych ocen ryzyka i wdrażanie środków łagodzących zidentyfikowane ryzyka.

Zapewnienie zgodności z przepisami o ochronie danych poprzez ciągłe monitorowanie i aktualizowanie praktyk ochrony danych.

Metody dydaktyczne

prezentacja informacyjna, dyskusja z rozwiązywaniem problemów, 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 qualitology 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