KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Ochrona danych [S2IBiJ1-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
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
15

Laboratorium
0

Inne
0

Ćwiczenia
15

Projekty/seminaria
0

Liczba punktów ECTS

2,00

Koordynatorzy

dr inż. Marek Goliński
marek.golinski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student posiada podstawową wiedzę1 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 przedsiebiorcom 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 ogranizacjach 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 informacyno-komunikacyjne charakterystyczne dla środowiska zawodowego związanego z zarządzaniem i ochroną danych w organizacjach [K2_U02].
2. Student potrafi dobrać i zastosować narzędzia komputerowego wspomagania rozwiązywania problemów charakterystycznych dla zarządzania sferą ochrony danych w ogranizacjach [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:

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- 10pytań, 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
Prawo ochrony danych osobowych to zbiór przepisów regulujących sposób, w jaki dane osobowe są zbierane, przetwarzane, przechowywane i udostępniane. Geneza tego prawa sięga lat 70. XX wieku, kiedy rozwój technologii informatycznych zaczął stanowić zagrożenie dla prywatności jednostek. Kluczowe źródła

prawa ochrony danych osobowych obejmują Rozporządzenie Ogólne o Ochronie Danych (RODO) w Unii Europejskiej oraz krajowe ustawy o ochronie danych osobowych. Te akty prawne mają na celu zapewnienie, że dane osobowe są przetwarzane zgodnie z prawem i w sposób chroniący prawa i wolności jednostek.

Definicja danych osobowych, ich rodzaje i szczególne kategorie
Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Mogą obejmować takie informacje jak imię i nazwisko, adres, numer PESEL, adres e-mail, a także bardziej wrażliwe dane, takie jak informacje o zdrowiu, orientacji seksualnej czy poglądach politycznych. Szczególne kategorie danych osobowych, zwane również danymi wrażliwymi, to informacje, które mogą narażać prywatność jednostki na szkodę i dlatego są objęte specjalną ochroną prawną.

Zasady przetwarzania danych osobowych "wrażliwych" i "zwykłych"
Przetwarzanie danych osobowych musi odbywać się zgodnie z określonymi zasadami, takimi jak:

Legalność: przetwarzanie danych musi mieć podstawę prawną.
Celowość: dane powinny być zbierane dla konkretnych, wyraźnych i prawnie uzasadnionych celów.
Minimalizacja danych: przetwarzane dane muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne.
Dokładność: dane muszą być prawidłowe i w razie potrzeby aktualizowane.
Integralność i poufność: dane muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo.
Dane "zwykłe" mogą być przetwarzane na podstawie zgody osoby, której dotyczą, lub innych przesłanek prawnych, takich jak wykonanie umowy czy obowiązek prawny. Dane "wrażliwe" mogą być przetwarzane tylko w wyjątkowych przypadkach, takich jak wyraźna zgoda osoby, której dotyczą, lub konieczność ochrony żywotnych interesów tej osoby.

Powierzenie przetwarzania danych a udostępnianie danych
Powierzenie przetwarzania danych polega na przekazaniu danych osobowych do innego podmiotu, który będzie je przetwarzał w imieniu administratora danych. Udostępnianie danych to przekazywanie danych osobowych innemu podmiotowi, który staje się odrębnym administratorem tych danych. Powierzenie przetwarzania wymaga zawarcia umowy powierzenia, która określa warunki i zasady przetwarzania danych przez podmiot przetwarzający.

Prawa osób, których dane poddawane są przetwarzaniu
Osoby, których dane są przetwarzane, mają szereg praw, w tym:

Prawo do informacji: prawo do wiedzy, jak ich dane są przetwarzane.
Prawo dostępu do danych: prawo do uzyskania kopii swoich danych.
Prawo do sprostowania danych: prawo do poprawienia nieprawidłowych danych.
Prawo do usunięcia danych (prawo do bycia zapomnianym): prawo do żądania usunięcia danych w określonych przypadkach.
Prawo do ograniczenia przetwarzania: prawo do ograniczenia przetwarzania danych w określonych sytuacjach.
Prawo do przenoszenia danych: prawo do przeniesienia danych do innego administratora.
Prawo do sprzeciwu wobec przetwarzania: prawo do sprzeciwu wobec przetwarzania danych na określonych warunkach.
Administrator danych ma obowiązek zapewnić możliwość realizacji tych praw.

Obowiązki administratora i podmiotu przetwarzającego dane
Administrator danych ma obowiązek zapewnić zgodność przetwarzania danych z przepisami prawa, w tym zapewnić odpowiednie środki techniczne i organizacyjne dla ochrony danych. Podmiot przetwarzający dane musi przetwarzać dane wyłącznie na zlecenie administratora i zgodnie z jego instrukcjami. Oba podmioty muszą prowadzić rejestr czynności przetwarzania oraz zgłaszać naruszenia ochrony danych do organu nadzorczego i, w niektórych przypadkach, do osób, których dane dotyczą.

Wyznaczanie, status i zadania inspektora ochrony danych
Inspektor ochrony danych (IOD) to osoba odpowiedzialna za nadzorowanie przestrzegania przepisów o ochronie danych osobowych w organizacji. IOD monitoruje przestrzeganie przepisów, doradza w kwestiach związanych z ochroną danych, szkoli personel, prowadzi audyty, współpracuje z organem nadzorczym

oraz pełni funkcję punktu kontaktowego dla osób, których dane są przetwarzane.

Zapewnienie zgodności i dokumentacja ochrony danych osobowych
Zapewnienie zgodności z przepisami o ochronie danych osobowych wymaga prowadzenia odpowiedniej dokumentacji, takiej jak polityki ochrony danych, procedury przetwarzania, rejestry czynności przetwarzania oraz oceny ryzyka. Organizacje muszą także przeprowadzać regularne audyty i szkolenia personelu w zakresie ochrony danych.

Ocena ryzyka
Ocena ryzyka to proces identyfikacji i analizy potencjalnych zagrożeń dla bezpieczeństwa danych osobowych oraz wdrażania środków zaradczych w celu minimalizacji tych ryzyk. Ocena ryzyka pomaga organizacjom zrozumieć, jakie są najważniejsze zagrożenia dla ochrony danych i jakie działania należy podjąć, aby zapewnić odpowiedni poziom bezpieczeństwa.

Ćwiczenia
Case Study - Procesy przetwarzania danych osobowych w firmie
Ćwiczenia w formie studium przypadku obejmują analizę i ocenę procesów przetwarzania danych osobowych w konkretnej firmie. Uczestnicy zapoznają się z praktycznymi aspektami przetwarzania danych, identyfikują potencjalne problemy i proponują rozwiązania zgodne z przepisami o ochronie danych osobowych. Analiza obejmuje cały cykl życia danych osobowych, od momentu ich zbierania, przez przechowywanie, aż po usuwanie.

Rodzaje dokumentów związanych z wybranymi procesami przetwarzania danych w firmie
Ćwiczenia te koncentrują się na różnych typach dokumentów, które są niezbędne do prawidłowego zarządzania procesami przetwarzania danych osobowych w firmie. Uczestnicy uczą się tworzyć i zarządzać dokumentacją, która obejmuje:

Umowa o dzieło/zlecenie: dokumenty regulujące współpracę z wykonawcami zewnętrznymi, które mogą obejmować klauzule dotyczące przetwarzania danych osobowych.
Umowa powierzenia przetwarzania danych osobowych: umowy między administratorem danych a podmiotem przetwarzającym, które określają zasady i warunki przetwarzania danych w imieniu administratora.
Zgoda na wykorzystanie wizerunku: dokumenty, które pozwalają firmie na legalne używanie wizerunku pracowników lub klientów do celów marketingowych lub promocyjnych.
Przetwarzanie danych zwykłych i sensytywnych: procedury i polityki dotyczące różnic w przetwarzaniu danych zwykłych (np. imię, nazwisko, adres) i sensytywnych (np. dane zdrowotne, dane biometryczne).
Ochrona danych osobowych w miejscu pracy
Ćwiczenia obejmują analizę polityk i procedur dotyczących ochrony danych osobowych pracowników w miejscu pracy. Uczestnicy uczą się, jak firmy powinny zarządzać danymi osobowymi pracowników, jakie środki bezpieczeństwa wdrażać oraz jakie prawa mają pracownicy w kontekście ochrony ich danych osobowych.

Ochrona i bezpieczeństwo danych osobowych z punktu widzenia osoby fizycznej i osoby prawnej, z uwzględnieniem wyzwań wynikających z funkcjonowania w świecie 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 Polskiejz 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 sprawieochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnegoprzepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochroniedanych).

3. Ustawa o ochronie danych osobowychz 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	30	1,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	20	0,50