

Zintegrowany Rejestr Kwalifikacji

Formularz dla kwalifikacji - podgląd

Typ wniosku

Wniosek o włączenie kwalifikacji do ZSK

Nazwa kwalifikacji*

Realizowanie zadań związanych z ochroną danych osobowych

Skrót nazwy

Rodzaj kwalifikacji*

kwalifikacja cząstkowa

Proponowany poziom Polskiej Ramy Kwalifikacji*

6

Krótką charakterystyka kwalifikacji, obejmująca informacje o działaniach lub zadaniach, które potrafi wykonywać osoba posiadająca tę kwalifikację oraz orientacyjny koszt uzyskania dokumentu potwierdzającego otrzymanie danej kwalifikacji*

Osoba posiadająca kwalifikację "Realizowanie zadań związanych z ochroną danych osobowych" jest przygotowana do opracowywania, wdrażania oraz nadzorowania systemów ochrony danych osobowych zgodnie z obowiązującymi przepisami krajowymi, europejskimi i pozaeuropejskimi w różnego rodzaju organizacjach, które przetwarzają dane osobowe. Osoba posiadająca kwalifikację może znaleźć zatrudnienie w jednostkach sektora finansów publicznych, instytutach badawczych, Narodowym Banku Polskim, w podmiotach prywatnych, które ze względu na regularne i systematyczne monitorowanie osób, których dane dotyczą, na dużą skalę, mają obowiązek, zgodnie z Art. 37 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), wyznaczenia inspektora danych osobowych (IOD), w podmiotach, których główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz w innych podmiotach prywatnych, które poszukują wsparcia przy administrowaniu danymi osobowymi. Orientacyjny nakład pracy potrzebny do uzyskania kwalifikacji został oszacowany na 104 godziny, w tym przykładowo 34 godziny na szkolenie/kurs lub inne formy uczenia się i 70 godzin czasu pracy własnej. Koszt dokumentu potwierdzającego kwalifikację wynosi 3000 zł netto.

Orientacyjny nakład pracy potrzebny do uzyskania kwalifikacji [godz.]*

104

Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji*

Uzyskaniem kwalifikacji „Realizowanie zadań związanych z ochroną danych osobowych” mogą być zainteresowani: - inspektorzy ochrony danych osobowych, którzy nie posiadają formalnie potwierdzonych kwalifikacji; - specjaliści ds. bezpieczeństwa informacji, bezpieczeństwa IT, audytorzy, prawnicy, którzy chcą zajmować się ochroną danych osobowych; - osoby delegowane do pełnienia funkcji inspektora ochrony danych osobowych w podmiotach administracji publicznej, zakładach opieki zdrowotnej i innych jednostkach zobowiązanych do wyznaczenia inspektora ochrony danych osobowych; - pracownicy i właściciele podmiotów prywatnych przetwarzających dane osobowe na szeroką skalę (banków, mediów społecznościowych, sklepów internetowych itd.) oraz wszystkich innych podmiotów prywatnych, które przetwarzają dane osobowe.

Wymagane kwalifikacje poprzedzające

Opis

Kwalifikacja pełna z poziomem 4 PRK

Lista

W razie potrzeby warunki, jakie musi spełniać osoba przystępująca do walidacji*

Kwalifikacja pełna z poziomem 4 PRK

Zapotrzebowanie na kwalifikację*

W związku z wdrożeniem z dniem 25 maja 2018 roku rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. L nr 119 z 4.05.2016 r., s. 1)[1] pojawia się ogromne zapotrzebowanie na osoby posiadające kwalifikację „Realizowanie zadań związanych z ochroną danych osobowych”, które mogą pełnić funkcję inspektora ochrony danych (IOD), ułatwiając przestrzeganie RODO. Kary pieniężne za naruszenia ochrony danych osobowych mogą sięgać kwot nawet 20 mln euro lub 4 proc. wartości rocznego światowego obrotu przedsiębiorstwa, co powoduje, że obowiązek wdrożenia RODO stał się jednym z najbardziej istotnych obowiązków dla firm i instytucji. Zapotrzebowanie na usługi związane z ochroną danych osobowych znacznie wzrosło od momentu wejścia w życie przepisów RODO, a na rynku potrzebni są specjaliści z fachową wiedzą w zakresie ochrony danych osobowych, znający realia przetwarzania danych w danej branży. Włączenie kwalifikacji do ZSK przyczyni się do profesjonalizacji usług świadczonych przez inspektorów ochrony danych. Na rynku istnieje zarówno wiele ofert szkoleń z zakresu ochrony danych osobowych, jak i samych ofert pochodzących od specjalistów, jednak są bardzo zróżnicowane pod względem poziomu oferowanych usług. Wyznaczenie inspektora ochrony danych jest obowiązkiem administratorów danych osobowych oraz podmiotów przetwarzających dane osobowe, będących organami lub podmiotami publicznymi (z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości), co oznacza, że każda instytucja publiczna, w tym wszystkie jednostki samorządu terytorialnego oraz ich jednostki budżetowe, takie jak szkoły, pomoc społeczna, straż pożarna, mają obowiązek powołania specjalisty przygotowanego do administrowania danymi osobowymi, przede wszystkim zaś - zapewnienia bezpieczeństwa danych. Obowiązek wyznaczenia osoby administrującej danymi w samych instytucjach publicznych posiada ponad 28 000 szkół, ponad 21 000 punktów przedszkolnych i przedszkoli[2], 957 szpitali[3], 13 839 oddziałów bankowych[4], 2808 jednostek samorządu terytorialnego[5], co daje 66 604 podmioty zobowiązane do wdrażania i stosowania procedur ochrony danych. O skali przetwarzania danych świadczą chociażby dane z branży finansowej - na koniec III kw. 2017 roku

banki obsługiwały 45,5 mln klientów, 31,5 mln prowadziło rachunki osobiste, a 15,6 mln aktywnie korzystało z bankowości według raportu „Polska bankowość w liczbach” opublikowanego przez PRNews.pl.[6] Podobny obowiązek ciąży na administratorze lub podmiocie przetwarzającym dane osobowe, którego główna działalność polega na operacjach przetwarzania, wymagających regularnego i systematycznego monitorowania osób na dużą skalę, co oznacza, że wiele przedsiębiorstw komercyjnych, w tym także firm prowadzących rozbudowaną działalność w internecie, polegającą na profilowaniu użytkowników, jest zobowiązanych do wprowadzenia polityki i procedur administrowania i ochrony danych osobowych. Dla określenia kategorii odbiorców powyższego obowiązku można posłużyć się kodem PKD 63.11.Z Przetwarzanie danych; zarządzanie stronami internetowymi (hosting) i podobna działalność. Podklasa ta obejmuje: przetwarzanie danych, włączając kompletną obróbkę i specjalistyczne raporty z danych dostarczonych przez klienta lub zapewnienie automatycznego przetwarzania danych oraz wprowadzania danych, włącznie z prowadzeniem bazy danych. Oznacza to, że z dużym prawdopodobieństwem można przyjąć założenie, iż aktywne podmioty gospodarcze, których przeważająca działalność to przetwarzanie danych na dużą skalę, są zobowiązane do wyznaczenia inspektora ochrony danych. Według szacunków Centralnej Ewidencji Informacji Działalności Gospodarczej takich podmiotów jest 122 617[7]. Trzecią grupę podmiotów związanych z przywołanym powyżej obowiązkiem stanowią firmy przetwarzające szczególne kategorie danych osobowych - tzw. dane wrażliwe (m.in. dotyczące zdrowia), o ile przetwarzają je na dużą skalę, np. szpitale. Obowiązek wyznaczenia inspektora ochrony danych posiadają także administratorzy danych osobowych (czyli właściciele firm, osoby uprawnione do reprezentacji), których główna działalność polega na przetwarzaniu na dużą skalę danych osobowych dotyczących wyroków skazujących i naruszeń prawa. Tak naprawdę jednak, każdy administrator danych osobowych, a więc każdy podmiot gospodarczy, nawet mała firma, powinien dokonać analizy, czy spełnia kryteria wskazane powyżej i w związku z tym, czy ma obowiązek wyznaczenia inspektora. Tymczasem rozporządzenie w sprawie ochrony osób fizycznych (RODO) w bardzo ogólny sposób opisuje kwalifikacje przyszłych inspektorów ochrony danych. Przepis art. 37 ust. 5 RODO wskazuje jedynie, że inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, przypisanych inspektorowi. W wytycznych Grupy Roboczej art. 29, dotyczących inspektorów ochrony danych wskazane są następujące kompetencje, którymi powinien charakteryzować się inspektor: ● wiedza na temat krajowych i europejskich przepisów i praktyk w zakresie ochrony danych, w tym dogłębnego zrozumienia RODO, ● zrozumienie przeprowadzanych procesów przetwarzania danych; ● zrozumienie technologii informacyjnych i bezpieczeństwa danych; ● znajomość sektora biznesowego i organizacji; ● umiejętność promowania kultury ochrony danych w organizacji. Wprawdzie art. 37(5) RODO nie wskazuje konkretnych kwalifikacji zawodowych, jakie należy brać pod uwagę wyznaczając inspektora ochrony danych, to jednak należy wskazać, że istotne jest, by posiadał on odpowiednią wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych i praktyk, jak również dogłębną znajomość RODO. Podmiotem zobowiązanym do stosowania RODO jest każdy przedsiębiorca, również prowadzący jednoosobową działalność gospodarczą, który przetwarza (choćby tylko pozyskuje i posiada) dane osobowe osób fizycznych w związku z działalnością zawodową, a więc trudno sobie wyobrazić przedsiębiorcę, który będzie zwolniony z tego obowiązku. Na koniec czerwca 2015 r. Główny Urząd Statystyczny oszacował liczbę podmiotów gospodarki narodowej na 4 155 328, w tym 4 017 103 to podmioty prywatne[8]. Można zatem przyjąć, że w Polsce ponad 4 miliony przedsiębiorców jest zobowiązanych do stosowania RODO oraz co najmniej 66 604 podmioty, będące organem lub instytucją publiczną. O tym, jak duże jest społeczne zapotrzebowanie na określenie kwalifikacji „Realizowanie zadań związanych z ochroną danych osobowych” świadczy szeroka oferta komercyjnych szkoleń i studiów podyplomowych, kształcących przyszłych

inspektorów/administratorów danych osobowych, jaka pojawiła się w ostatnim czasie w związku z wejściem w życie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. L nr 119 z 4.05.2016 r., s. 1) - na dzień 29 czerwca 2018 dostępnych jest 4229 usług rozwojowych dotyczących RODO[9]”. Oferta programowa, zakres szkolenia i oferowane programy są bardzo zróżnicowane i niejednolite. Tymczasem w interesie bardzo obszernej grupy odbiorców, zobowiązanych z mocy prawa do wyznaczenia odpowiedniego inspektora ochrony danych osobowych, jest powierzenie tego ważnego zadania, jakim jest bezpieczeństwo danych osobowych osób fizycznych, osobie profesjonalnie do tego zadania przygotowanej, co będzie potwierdzała ta kwalifikacja. Włączenie kwalifikacji „Realizowanie zadań związanych z ochroną danych osobowych” przyczyni się zarówno do wypracowania standardu kompetencji osób, które zajmują się ochroną danych po stronie prywatnych podmiotów i instytucji publicznych, jak również do wzrostu świadomości i kultury ochrony danych.

[1] 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)

https://giodo.gov.pl/234/id_art/9276/j/pl

[2]https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5501/14/10/1/polska_w_liczbach_2017.pdf [3]

<http://www.portalsamorzadowy.pl/ochrona-zdrowia/liczba-szpitali-w-województwach-polsce-gus-o-ochronie-zdrowia,102313.html> [4]

<https://prnews.pl/raport-prnews-pl-liczba-placowek-bankowych-iii-kw-2017-431565> [5]

<http://administracja.mswia.gov.pl/adm/baza-jst/baza-teleadresowa-jst-d/7788,Baza-teleadresowa-JST-do-pobrania.html> [6]

https://www.bankier.pl/static/att/166000/7563298_raport_bankowosc_iii_kw2017.pdf [7]

<https://prod.ceidg.gov.pl/CEIDG/CEIDG.Public.UI/Search.aspx>; dane na dzień 28 czerwca 2018 r.

[8] http://www.coig.com.pl/spis-polskich-firm_katalog_polskich_firm.php [9]

<https://uslugirozwojowe.parp.gov.pl/uslugi/search?ServicesSearchForm%5Bfraz%5D=rodo>

Odniesienie do kwalifikacji o zbliżonym charakterze oraz wskazanie kwalifikacji ujętych w ZRK zawierających wspólne zestawy efektów uczenia się*

Część efektów uczenia się właściwa dla kwalifikacji może być wspólna z efektami uczenia się na studiach podyplomowych na kierunkach „Inspektor ochrony danych”. Charakter efektów uczenia się jest na tyle różny, że bezpośrednie odniesienie ich do efektów uczenia się wymaganych dla kwalifikacji „Realizowanie zadań związanych z ochroną danych osobowych” nie jest zasadne. Kwalifikacja ukierunkowana jest na praktyczne umiejętności związane z identyfikowaniem procesów przetwarzania danych osobowych, sporządzaniem dokumentacji ochrony danych, monitorowaniem zgodności procesów przetwarzania danych osobowych z obowiązującymi przepisami oraz współpracą z organem nadzorczym. W kwalifikacji uwzględniono także nieujęte w kwalifikacjach z systemu szkolnictwa wyższego umiejętności związane z wykorzystaniem technologii informacyjnych w procesach przetwarzania danych osobowych. Należy podkreślić, że w ramach systemu szkolnictwa wyższego posiadanie efektów uczenia się, pokrywających się zakresem z opisaną kwalifikacją rynkową, nie może zostać potwierdzone w całości w wyniku walidacji uczenia się pozaformalnego i nieformalnego. Włączenie kwalifikacji do ZSK umożliwi potwierdzenie kompetencji przez osoby, które chcą skorzystać z równoważnej do formalnej ścieżki uczenia się przez całe życie.

Typowe możliwości wykorzystania kwalifikacji*

Osoba posiadająca kwalifikację „Realizowanie zadań związanych z ochroną danych osobowych” może znaleźć zatrudnienie w: ● w jednostkach sektora finansów publicznych, do których zaliczają się organy władzy publicznej, tj. jak organy administracji rządowej, organy kontroli państwowej i ochrony prawa, ZUS, jednostki samorządu terytorialnego, ale także uczelnie publiczne, PAN, państwowe i samorządowe instytucje kultury ● instytutach badawczych; ● Narodowym Banku Polskim; ● w podmiotach prywatnych, które ze względu na regularne i systematyczne monitorowanie osób, których dane dotyczą, na dużą skalę, mają obowiązek wyznaczenia IOD (banki, media społecznościowe, sklepy internetowe, podmioty korzystające z tzw. „kart miejskich”, prowadzące monitoring wizyjny na szeroką skalę); ● w podmiotach, których główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych (np. szpitale i inne zakłady opieki zdrowotnej); ● w innych podmiotach prywatnych, które poszukują wsparcia przy administrowaniu danymi osobowymi.

Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację*

1. Etap weryfikacji 1.1. Metody Weryfikacja składa się z dwóch etapów: części teoretycznej i części praktycznej. W części teoretycznej wykorzystuje się metodę testu teoretycznego. W części praktycznej stosuje się wyłącznie następujące metody weryfikacji: obserwacja w warunkach symulowanych (symulacja), wywiad ustrukturyzowany (rozmowa z komisją), a także analiza dowodów i deklaracji wyłącznie na etapie przedłużania ważności certyfikatu. 1.2. Zasoby kadrowe W procesie walidacji biorą udział: ● w przypadku, gdy test teoretyczny przeprowadzany jest w elektronicznym systemie - operator systemu egzaminacyjnego, który organizuje zaplecze techniczne do przeprowadzenia weryfikacji i nadzoruje przebieg testu. Natomiast, gdy test przeprowadzany jest poza systemem elektronicznym należy zapewnić nadzór nad prawidłowym przebiegiem tej części walidacji; ● komisja walidacyjna, składająca się z co najmniej 2 asesorów, która przeprowadza część praktyczną oraz w przypadku, gdy test przeprowadzany poza systemem elektronicznym, odpowiada za sprawdzenie testu. Osoba będąca asesorem może być jednocześnie operatorem systemu egzaminacyjnego i osobą nadzorującą przebieg testu teoretycznego prowadzonego poza systemem elektronicznym. Operator systemu egzaminacyjnego musi posiadać: - wykształcenie minimum średnie, - znajomość obsługi komputera w zakresie uruchamiania oraz podstawowej obsługi systemu i zainstalowanych aplikacji, - umiejętność rozwiązywania problemów w sytuacji trudności z nawiązaniem lub zanikiem połączenia internetowego lub obsługą przeglądarki w zakresie kompatybilności z platformą egzaminacyjną. Weryfikację efektów uczenia się w części praktycznej prowadzi komisja walidacyjna, składająca się z min. 2 osób. Każdy członek komisji walidacyjnej: - musi posiadać kwalifikację pełną z poziomem co najmniej 4 PRK; - musi posiadać udokumentowane doświadczenie w zakresie wdrażania RODO w organizacjach (minimum 5 wdrożeń) lub - musi pełnić obecnie funkcję inspektora ochrony danych lub w przeszłości funkcję administratora bezpieczeństwa informacji przez minimum 3 lata; - przeprowadził minimum 50 godzin szkoleń wewnętrznych lub otwartych w zakresie ochrony danych osobowych. Do zadań członków komisji należy m.in.: - stosowanie kryteriów weryfikacji przypisanych do efektów uczenia się dla opisywanej kwalifikacji oraz kryteriów oceny formalnej i merytorycznej dowodów na posiadanie efektów uczenia się właściwych dla opisywanej kwalifikacji; - stosowanie zasad prowadzenia weryfikacji, a także różnych metod weryfikacji efektów uczenia się, zgodnie z celami walidacji i zasadami Zintegrowanego Systemu Kwalifikacji. Jeżeli instytucja certyfikująca prowadzi kształcenie w obszarze wnioskowanej kwalifikacji to musi stosować rozwiązania zapewniające rozdzielanie procesów kształcenia i szkolenia od walidacji. W szczególności istotne jest zapewnienie bezstronności osób przeprowadzających walidację m.in poprzez rozdział osobowy mający na celu zapobieganie konfliktowi interesów osób przeprowadzających walidację. Osoby te

nie mogą weryfikować efektów uczenia się osób, które były przez nie przygotowywane do uzyskania kwalifikacji „Realizowanie zadań związanych z ochroną danych osobowych”. 1.3. Sposób organizacji walidacji oraz warunki organizacyjne i materialne Instytucja certyfikująca musi zapewnić: ● (w przypadku, gdy test teoretyczny przeprowadzany jest w elektronicznym systemie) stanowisko komputerowe dla kandydata ubiegającego się o nadanie kwalifikacji (jedno stanowisko dla jednego kandydata), wyposażone w przeglądarkę internetową z dostępem do internetu) do realizacji części teoretycznej walidacji; ● stanowisko biurowe wraz z przyborami (np.flipchart, flamastry, długopis, brudnopis); ● wydrukowane rozporządzenie RODO, wytyczne grupy roboczej art. 29 dotyczące inspektorów ochrony danych dla każdego kandydata; ● wydrukowaną Ustawę o ochronie danych osobowych; ● wydrukowane wnioski zgłoszenia naruszeń ochrony danych osobowych do organu nadzorczego; ● case study do weryfikacji efektów uczenia się w ramach Zestawu 3 “Wspieranie administratora w budowaniu systemu ochrony danych osobowych” powinien dotyczyć małej firmy, zatrudniającej do 5 osób. Instytucja certyfikująca musi zapewnić bezstronną i niezależną procedurę odwoławczą, w ramach której osoby uczestniczące w procesie walidacji i certyfikacji, mają możliwość odwołania się od decyzji dotyczących spełnienia wymogów formalnych, samych wyników, a także decyzji kończącej walidację. W przypadku negatywnego wyniku walidacji instytucja prowadząca walidację jest zobowiązana przedstawić uzasadnienie decyzji. 2. Etapy identyfikowania i dokumentowania Nie określa się wymagań.

Propozycja odniesienia do poziomu sektorowych ram kwalifikacji (o ile dotyczy)

Nie dotyczy

Syntetyczna charakterystyka efektów uczenia się*

Osoba posiadająca kwalifikację „Realizowanie zadań związanych z ochroną danych osobowych” jest przygotowana do samodzielnego opracowywania oraz wdrażania systemów ochrony danych osobowych w różnych organizacjach przetwarzających dane z uwzględnieniem obowiązujących przepisów krajowych, europejskich i pozaeuropejskich. Identyfikuje możliwe procesy przetwarzania danych osobowych w organizacji oraz ich przepływy, szacuje ryzyko naruszenia ochrony danych osobowych oraz ocenia bezpieczeństwo procesu przetwarzania danych osobowych, sporządza podstawową dokumentację ochrony danych. Przeprowadza audyty zgodności procesów przetwarzania danych osobowych z RODO. Reprezentuje interesy administratora przed organem nadzorczym oraz osobami, których dane są przetwarzane przez daną organizację. Identyfikuje minimalne wymogi bezpieczeństwa dotyczące ochrony danych osobowych w technologiach informacyjnych oraz dobiera niezbędne elementy budowy systemu informatycznego umożliwiające bezpieczne przetwarzanie danych osobowych.

Zestawy efektów uczenia się

Numer zestawu w kwalifikacji*

1

Nazwa zestawu*

Posługiwanie się wiedzą w zakresie krajowych, europejskich i pozaeuropejskich przepisów o ochronie danych osobowych

Poziom PRK*

5

Orientacyjny nakład pracy [godz.]*

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia*

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

Efekt uczenia się

Charakteryzuje przepisy krajowe dotyczące ochrony danych osobowych

Kryteria weryfikacji*

- wymienia akty prawne regulujące ochronę danych osobowych w Polsce; - wskazuje zatwierdzone kodeksy postępowania dotyczące dobrych praktyk w zakresie ochrony danych osobowych w poszczególnych branżach i zasadność ich stosowania; - omawia rolę i zadania polskiego organu nadzorczego w zakresie ochrony danych osobowych; - wskazuje i omawia odmienne regulacje, wyłączenia i uszczegółowienia przepisów krajowych w odniesieniu do RODO; - charakteryzuje zasady postępowania w sytuacji naruszenia przepisów o ochronie danych osobowych; - omawia zasady odpowiedzialności cywilnej i karnej za naruszenie przepisów o ochronie danych osobowych.

Efekt uczenia się

Omawia pozaeuropejskie przepisy o ochronie danych osobowych

Kryteria weryfikacji*

- definiuje pojęcia: tarcza prywatności, klauzule umowne; - omawia zasady transgranicznego przetwarzania danych poza obszarem EOG; - omawia zasady stosowania tarczy prywatności; - omawia konieczność stosowania klauzul umownych.

Efekt uczenia się

Omawia rozporządzenie ogólne o ochronie danych osobowych nr 2016/679 (RODO)

Kryteria weryfikacji*

- definiuje pojęcia: dane osobowe, przetwarzanie, zbiór danych, administrator, współadministrowanie danych, odbiorca danych, procesor, podmiot przetwarzający, organ nadzorczy, profilowanie, pseudonimizacja, podmiot wiodący, kontekst przetwarzania; - wyjaśnia skróty: RODO, motyw RODO, PUODO, DPO, IOD, ADO, DPIA; - charakteryzuje zasady przetwarzania danych osobowych wynikające z RODO (np. minimalizacji danych, prywatności w fazie projektowania, domyślnej ochrony danych); - omawia podstawy prawne przetwarzania danych osobowych (zgoda, wykonanie lub zawarcie umowy, obowiązek prawny, żywotne interesy, interes publiczny lub sprawowanie władzy publicznej, uzasadnione interesy administratora), w tym danych szczególnej kategorii zgodnie z art. 9 RODO; - omawia zasady transgranicznego przetwarzania danych w ramach EOG; - omawia prawa osób, których dane dotyczą (np. prawo do bycia zapomnianym, wycofanie zgody); - charakteryzuje obowiązki administratora i podmiotu przetwarzającego; - omawia status, rolę i zadania inspektora danych osobowych; - wskazuje skutki naruszeń ochrony danych osobowych; - wymienia źródła oficjalnych interpretacji i wyjaśnień treści RODO (wytyczne

Grupy Roboczej Art.29).

Numer zestawu w kwalifikacji*

2

Nazwa zestawu*

Posługiwanie się wiedzą z zakresu wykorzystania technologii informacyjnych w procesach przetwarzania danych osobowych

Poziom PRK*

6

Orientacyjny nakład pracy [godz.]*

14

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia*

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

Efekt uczenia się

Charakteryzuje zasady dostępu do systemów i aplikacji

Kryteria weryfikacji*

- omawia procedury nadawania dostępu do systemów informatycznych; - omawia zasady prawidłowości realizacji obowiązków administratora w zakresie nadawania uprawnień do systemów informatycznych.

Efekt uczenia się

Omawia zasady bezpieczeństwa w zakresie technologii informacyjnych

Kryteria weryfikacji*

- identyfikuje minimalne wymogi bezpieczeństwa dotyczące ochrony systemu informatycznego (np. szyfrowanie); - dobiera do wymogów bezpieczeństwa niezbędne elementy budowy systemu informatycznego służącego do bezpiecznego przetwarzania danych osobowych (np. certyfikat szyfrujący); - charakteryzuje elementy profilowania i zautomatyzowanego podejmowania decyzji; - wymienia obowiązki administratora związane ze zautomatyzowanym podejmowaniem decyzji.

Numer zestawu w kwalifikacji*

3

Nazwa zestawu*

Wspieranie administratora w budowaniu systemu ochrony danych osobowych

Poziom PRK*

6

Orientacyjny nakład pracy [godz.]*

48

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia*

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

Efekt uczenia się

Diagnostuje przepływ danych osobowych

Kryteria weryfikacji*

- wymienia obowiązkowe elementy umowy powierzenia danych; - wskazuje dopuszczalne formy zawarcia umowy powierzenia danych; - weryfikuje zgodność podmiotu przyjmującego dane z przepisami RODO; - wskazuje różnice między powierzeniem a współadministrowaniem danymi osobowymi.

Efekt uczenia się

Identyfikuje procesy przetwarzania danych osobowych

Kryteria weryfikacji*

- przygotowuje formularz audytu zgodności przetwarzania danych osobowych z RODO; - określa kategorie, zakres i cele przetwarzania danych osobowych; - weryfikuje czy zakres danych jest adekwatny do celów przetwarzania danych; - określa miejsca przetwarzania danych; - określa odbiorców danych; - identyfikuje zabezpieczenia procesów przetwarzania danych osobowych.

Efekt uczenia się

Ocenia bezpieczeństwo procesu przetwarzania danych osobowych

Kryteria weryfikacji*

- rozróżnia i omawia techniczne i organizacyjne środki bezpieczeństwa procesu przetwarzania danych osobowych; - wskazuje różnice między pseudonimizacją a anonimizacją; - dokonuje analizy adekwatności doboru technicznych i organizacyjnych środków bezpieczeństwa do stwierdzonych ryzyk; - wskazuje uchybienia w technicznych i organizacyjnych środkach bezpieczeństwa.

Efekt uczenia się

Podejmuje działania mające na celu zwiększenie świadomości personelu uczestniczącego w operacjach przetwarzania ochrony danych osobowych

Kryteria weryfikacji*

- wyjaśnia rolę i zadania inspektora ochrony danych w organizacji; - przekłada pojęcia związane z ochroną danych osobowych na język zrozumiały dla administratora i osób, których dane dotyczą; - przygotowuje ramowy program szkolenia na temat znaczenia ochrony danych osobowych oraz roli i zadań administratora.

Efekt uczenia się

Sporządza dokumentację ochrony danych

Kryteria weryfikacji*

- wymienia minimalne elementy niezbędne do zbudowania polityki bezpieczeństwa ochrony danych; - redaguje klauzule informacyjne zgodnie z zasadą przejrzystości (art. 12 RODO); - redaguje klauzule zgód zgodnie z art. 6 i art. 7 ust.2 RODO; - wskazuje elementy rejestru czynności przetwarzania danych osobowych; - wskazuje elementy rejestru kategorii czynności przetwarzania danych osobowych.

Efekt uczenia się

Szacuje ryzyko naruszenia danych osobowych osób fizycznych i ocenia skutki przetwarzania dla ochrony danych

Kryteria weryfikacji*

- tworzy spis ryzyk zagrażających podmiotowi przetwarzającemu dane, mogących wystąpić w związku z przetwarzaniem danych osobowych w wersji elektronicznej oraz w wersji papierowej; - dokonuje oceny ryzyka z wykorzystaniem macierzy ryzyka; - udziela zaleceń co do oceny skutków dla ochrony danych; - rekomenduje sposoby postępowania z ryzykiem oraz uzasadnia ich zastosowanie.

Efekt uczenia się

Weryfikuje zgodność przetwarzania danych osobowych z prawem

Kryteria weryfikacji*

- określa charakter danych osobowych (wrażliwe, zwykłe); - wskazuje podstawę prawną przetwarzania danych osobowych; - opisuje możliwe uzasadnione interesy administratora jako podstawę przetwarzania danych; - uzasadnia dlaczego interesy administratora są nadrzędne w stosunku do interesów osób, których dane są przetwarzane.

Numer zestawu w kwalifikacji*

4

Nazwa zestawu*

Monitorowanie zgodności procesów przetwarzania danych osobowych z RODO

Poziom PRK*

6

Orientacyjny nakład pracy [godz.]*

12

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia*

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

Efekt uczenia się

Charakteryzuje elementy dokumentacji z naruszeń ochrony danych osobowych

Kryteria weryfikacji*

- wskazuje niezbędne elementy wchodzące w skład dokumentacji z naruszeń zgodnie z art. 33 ust. 5 RODO; - tłumaczy zasadność tworzenia rejestrów związanych z naruszeniem ochrony danych osobowych; - wskazuje termin zgłoszenia w zależności od wagi skutków naruszenia ochrony danych osobowych.

Efekt uczenia się

Identyfikuje incydenty z zakresu ochrony danych osobowych

Kryteria weryfikacji*

- wymienia przykładowe incydenty ochrony danych osobowych; - kwalifikuje incydent pod kątem zasadności zgłoszenia ochrony danych osobowych organowi nadzorcemu.

Efekt uczenia się

Przeprowadza audyt zgodności procesów przetwarzania danych osobowych z RODO

Kryteria weryfikacji*

- omawia zasady przeprowadzania audytów; - przygotowuje plan sprawdzeń oraz plan audytu zgodności procesów przetwarzania danych osobowych z RODO; - formułuje pytania do audytowanego; - identyfikuje oraz uzasadnia niezgodności w zakresie ochrony danych osobowych z obowiązującymi przepisami; - formułuje wnioski pokontrolne.

Numer zestawu w kwalifikacji*

5

Nazwa zestawu*

Współpraca z organem nadzorczym i reprezentowanie interesów administratora wobec organu nadzorczego i osób, których dane dotyczą

Poziom PRK*

6

Orientacyjny nakład pracy [godz.]*

8

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia*

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

Efekt uczenia się

Reprezentuje interesy administratora wobec organu nadzorczego i osób, których dane dotyczą

Kryteria weryfikacji*

- omawia zasady prowadzenia uprzednich konsultacji z organem nadzorczym zgodnie z art. 36 RODO; - identyfikuje przypadki konieczności konsultacji z organem nadzorczym; - przygotowuje przykładową odpowiedź na wniosek o bycie zapomnianym.

Efekt uczenia się

Sporządza zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego

Kryteria weryfikacji*

- wskazuje niezbędne elementy zgłoszenia naruszenia; - omawia tryb zgłaszania i obowiązujące terminy; - wypełnia przykładowe zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego.

Informacje o instytucjach uprawnionych do nadawania kwalifikacji

Wnioskodawca*

Fundacja VCC

Minister właściwy*

Ministerstwo Cyfryzacji

Okres ważności dokumentu potwierdzającego nadanie kwalifikacji i warunki przedłużenia jego ważności*

Certyfikat ważny 5 lat. Warunkiem przedłużenia certyfikatu jest wykonywanie zadań związanych z kwalifikacją przez minimum 3 lata od momentu uzyskania kwalifikacji.

Nazwa dokumentu potwierdzającego nadanie kwalifikacji*

Certyfikat

Uprawnienia związane z posiadaniem kwalifikacji*

Nie dotyczy

Kod dziedziny kształcenia*

34 - Gospodarka i administracja

Kod PKD*

Kod	Nazwa
63.11	Przetwarzanie danych; zarządzanie stronami internetowymi (hosting) i podobna działalność

Status

Dokumenty

#	Tytuł dokumentu
1	KRS rejestr przedsiębiorców
2	KRS rejestr stowarzyszeń
3	Potwierdzenie wniesienia opłaty
4	Statut
5	ZRK_FKU_Realizowanie zadań związanych z ochroną danych osobowych



Oświadczam, że dane zawarte we wniosku o włączenie kwalifikacji rynkowej do Zintegrowanego Systemu Kwalifikacji są zgodne z prawdą. Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia.*

Dane o podmiocie, który złożył wniosek

Fundacja VCC

Siedziba i adres: Matki Teresy z Kalkuty 18 lok.16, 20-538 Lublin

NIP: 7123281299

REGON: 061608116

Numer KRS: 0000479551

Reprezentacja: Radosław Panas - Prezes Zarządu, Edyta Migalka - Dyrektor ds. komunikacji

Adres elektroniczny osoby wnoszącej wniosek: edyta.migalka@vccsystem.eu