

DZIEŃ I – Przygotowanie do wdrożenia RODO. Jak przeprowadzić samodzielny audyt wymagań

10.00	OTWARCIE
10.00 – 10.45	<p style="text-align: center;">Aktualne wymogi prawne w zakresie ochrony danych osobowych. Czy tylko RODO?</p> <ul style="list-style-type: none"> - europejski system ochrony danych osobowych - system ochrony danych osobowych w Polsce - ustawy branżowe i ich rola w ochronie danych osobowych, - przepisy regulujące praw konsumenta a ich wpływ na ochronę danych osobowych - jawność życia publicznego a ochrona danych osobowych - dane osobowe a działalność administracji i projekty unijne - wpływ RODO na funkcjonowanie firm i instytucji
10.45 – 11.15	<p style="text-align: center;">Przygotowanie do przeprowadzenia audytu</p> <ul style="list-style-type: none"> - cel działań audytowych. Audyt jako podstawowa część wdrażających i monitorujących zgodność działań jednostki z RODO - ustalenie zakresu działań audytowych - przygotowanie zespołu audytowego - metodologia prowadzenia działań audytowych - harmonogram działań audytowych i czas ich realizacji
11.15 – 11.45	<p style="text-align: center;">Inwentaryzacja procesów przetwarzania danych osobowych dla potrzeb RODO</p> <ul style="list-style-type: none"> - dlaczego i jak szybko i sprawnie przeprowadzić inwentaryzację? - elementy inwentaryzacji procesów przetwarzania danych osobowych - jakie informacje i dane powinny być zebrane w czasie inwentaryzacji? - gdzie szukać procesów przetwarzania danych w firmie/instytucji? - wykorzystanie dotychczasowej dokumentacji oraz ewidencji w celu dokonania inwentaryzacji - mapa procesów i ewidencja danych na potrzeby audytu i monitorowania zgodności z RODO
11.45 – 12.15	<p style="text-align: center;">Określenie obowiązków, które dotyczą danego podmiotu na gruncie RODO</p> <ul style="list-style-type: none"> - obowiązki podmiotu jako administratora - obowiązki podmiotu jako processora - obowiązki podmiotu jako subprocessora - obowiązki podmiotu jako współadministratora
12.15 – 13.00	Obiad
13.00 – 14.30	<p style="text-align: center;">Działania audytowe w zakresie realizacji kluczowych obowiązków</p> <ul style="list-style-type: none"> - legalność przetwarzania danych – <i>sprawdzenie podstaw prawnych przetwarzania danych zwykłych i danych wrażliwych</i> - obowiązki informacyjne – <i>pierwotne i wtórne obowiązki informacyjne – zakres i sposób realizacji</i> - analiza w zakresie stosowania koncepcji ochrony danych w fazie projektowania – <i>formalne i proceduralne wdrożenie koncepcji w organizacji</i> - analiza w zakresie stosowania koncepcji domyślnej ochrony danych – <i>formalne i proceduralne wdrożenie koncepcji w organizacji</i> - ocena legalności i prawidłowości przy przekazywaniu danych – <i>powierzenie przetwarzania danych osobowych, udostępnianie danych, transfer danych do państw trzecich</i> - ocena ryzyka przetwarzania danych osobowych – <i>zakres i metodologia oceny ryzyka, dokumentacja oraz zastosowanie wyników dla potrzeb realizacji obowiązków</i> - ocena skutków dla ochrony danych (DPIA) – <i>sprawdzenie procedur prowadzenia DPIA, zakres DPIA, metodologia, dokumentowanie procesu i wyników</i> - naruszenie ochrony danych – <i>ocena procedur wewnętrznych oraz przygotowania do realizacji obowiązków w zakresie zgłaszania naruszeń do organu nadzoru i zawiadamiania osób, których dane dotyczą</i> - czasowość, poprawność, adekwatność – <i>badanie procedur oraz ich stosowania</i> - powołanie DPO – <i>analiza dotycząca formalnego powołania inspektora ochrony danych i jego kwalifikacji, zakresu obowiązków oraz organizacji stanowiska pracy</i>
14.30 – 15.00	<p style="text-align: center;">Działania audytowe w zakresie zabezpieczenia danych</p> <ul style="list-style-type: none"> - jak sprawdzić zabezpieczenie danych osobowych, gdy brak wyraźnych wymogów w RODO? - standardy – jakie standardy można wykorzystać do dokonania oceny? - zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe
15.00 – 15.30	<p style="text-align: center;">Działania audytowe w zakresie praw podmiotów danych</p> <p>badanie zasad przyjęcia wniosków/żądań, procedur dotyczących ich rozpatrzenia oraz realizacji wymogów formalnych odnoszących się do zakresu i sposobu realizacji poszczególnych praw podmiotów danych obejmujących:</p> <ul style="list-style-type: none"> - prawo dostępu do danych - prawo do sprostowania/uzupełnienia danych - prawo do ograniczenia przetwarzania - przenoszenie danych - prawo sprzeciwu - prawo do tego by nie podlegać profilowaniu - cofnięcie zgody
15.30 – 15.40	Przerwa
15.40 – 16.00	<p style="text-align: center;">Działania audytowe w zakresie dokumentacji przetwarzania danych wymaganej na gruncie RODO</p> <ul style="list-style-type: none"> - jakie dokumenty/procedury powinien mieć podmiot przetwarzający dane osobowe zgodnie z RODO? - inne dokumenty wewnętrzne - zasada rozliczalności – nowość na gruncie RODO
16.00 – 16.15	<p style="text-align: center;">Sposób przedstawiania i wykorzystywania wyników audytu w procesie badania zgodności z RODO</p> <ul style="list-style-type: none"> - raport / wyniki audytu – prezentacja wyników – WZORCOWY SZABLON
16.15 – 16.45	<p style="text-align: center;">Listy kontrolne w zakresie zgodności z RODO</p> <ul style="list-style-type: none"> - sprawdzenie prawidłowości konstrukcji zgód - konieczność powołania Inspektora Ochrony Danych - prawidłowość konstrukcji upoważnień, - retencja danych - polityka konfliktu interesów - procedury zawierania umów - zasady korespondencji elektronicznej
16.45	ZAKOŃCZENIE

DZIEŃ II - Analiza ryzyka zgodnie z RODO oraz określenie minimalnych standardów w zakresie zabezpieczeń danych osobowych

9.30 OTWARCIE	
9.30 – 10.00	Wymagania przepisów o ochronie danych osobowych w zakresie analizy ryzyka <ul style="list-style-type: none">- podstawy prawne wykonywania analizy ryzyka- czy każda firma/institucja jest zobligowana do przeprowadzania analizy ryzyka?- cel wykonywania analizy ryzyka- zespół ds. przeprowadzania analizy ryzyka- jak wybrać metodę analizy ryzyka?- kiedy i jak często przeprowadzać analizę ryzyka?- sposób dokumentowania wyników- zasady opracowywania i wdrażania procedury przeprowadzania analizy ryzyka
10.00 – 11.00	Ocena ryzyka naruszenia praw i wolności osób, których dane są przetwarzane <ul style="list-style-type: none">- proces zarządzania ryzykiem w organizacji- zarządzanie ryzykiem w kontekście ochrony danych osobowych i ocena skutków dla ochrony danych- zalecenia Europejskiej Rady ds. Ochrony Danych (EROD - dawna Grupa Robocza art 29)- zarządzanie ryzykiem zgodnie z ISO 31000/27001- metodyka SDM- metodyka PIA- praktyczne podejście do zarządzania ryzykiem w obszarze ochrony danych osobowych- identyfikacja środków zabezpieczających w oparciu o plan postępowania z ryzykiem
11.00 – 12.00	Minimalne standardy w zakresie zabezpieczenia danych osobowych <ul style="list-style-type: none">- kategorie technicznych i organizacyjnych środków zabezpieczających- podstawy normatywne w zakresie ochrony informacji- ochrona dostępu do danych- monitorowanie operacji na danych osobowych- ochrona infrastruktury sieciowej- wielopoziomowa ochrona integralności danych osobowych- szyfrowanie i pseudonimizacja- ochrona przed złośliwym oprogramowaniem- ochrona przed wyciekiem danych- zabezpieczenie pomieszczeń, w których odbywa się przetwarzanie danych osobowych
12.00 – 12.15	Przerwa
12.15 – 13.00	Zapewnienie odporności systemów i usług przetwarzania <ul style="list-style-type: none">- odporność na naruszenia bezpieczeństwa- zakres funkcjonalności- utwardzenie konfiguracji- środki zapobiegające naruszeniom bezpieczeństwa
13.00 – 13.45	Ciągłość przetwarzania i ochrony danych osobowych oraz zapewnienie możliwości ich odtworzenia <ul style="list-style-type: none">- odporność na naruszenia bezpieczeństwa- zakres funkcjonalności- utwardzenie konfiguracji- środki zapobiegające naruszeniom bezpieczeństwa
13.45 – 14.30	Obiad
14.30 – 15.15	Testowanie, weryfikacja i ocena poziomu bezpieczeństwa
15.15 – 15.30	Przerwa
15.30 – 16.15	Polityki ochrony danych <ul style="list-style-type: none">- zasady bezpiecznego przetwarzania danych- minimalne wymagania w zakresie bezpieczeństwa- zarządzanie ryzykiem- zarządzanie dostępem do danych- zarządzanie zmianami- zarządzanie podatnościami- incydenty naruszenia bezpieczeństwa danych osobowych
16.15 – 16.45	Ocena skutków dla ochrony danych osobowych <ul style="list-style-type: none">- wytyczne EROD i UODO w zakresie przeprowadzenia oceny skutków- narzędzia pomocne do wykonania oceny skutków dla przeprowadzenia oceny
16.45	ZAKOŃCZENIE

DZIEŃ III - Dokumentacja w zakresie ochrony danych osobowych

10.00		OTWARCIE
10.00 – 11.00	Dokumentacja w zakresie ochrony danych osobowych cz.1	<ul style="list-style-type: none">- Polityka bezpieczeństwa /regulamin ochrony danych osobowych/wytyczne w zakresie postępowania z danymi osobowymi- rejestr czynności przetwarzania oraz rejestr kategorii przetwarzania- treść obowiązku informacyjnego
11.00 - 11.45	Dokumentacja w zakresie ochrony danych osobowych cz.2 - umowy i upoważnienia, poufność	<ul style="list-style-type: none">- umowa powierzenia przetwarzania danych osobowych- klauzule umowne w zakresie ochrony danych osobowych- upoważnienia do przetwarzania danych osobowych- podpowierzenie przetwarzania danych osobowych- współadministrowanie danymi osobowymi - umowa- oświadczenie o poufności
11.45-12.00	Przerwa	
12.00-13.00	Dokumentacja w zakresie ochrony danych osobowych cz.3 - wykazy i rejestry	<ul style="list-style-type: none">- rejestr udostępnień danych osobowych- wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe,- wykaz umów powierzenia przetwarzania danych osobowych,- wykaz udostępnień osobom, których dane dotyczą- ewidencja osób upoważnionych do przetwarzania danych osobowych
13.00 - 14.00	Dokumentacja w zakresie ochrony danych osobowych cz. 4 - zgoda na przetwarzanie danych osobowych, analiza ryzyka i metodyka identyfikacji DPIA	<ul style="list-style-type: none">- zgoda na przetwarzanie danych osobowych,- analiza ryzyka i zagrożeń przetwarzania danych osobowych jako dokument- metodyka identyfikacji czynności przetwarzania danych wymagających DPIA- protokół naruszenia i zagrożenia ochrony danych osobowych- wymagania dla kontrahentów w zakresie zabezpieczenia ochrony danych osobowych
14.00 - 14.45	Obiad	
14.45 - 15.45	Dokumentacja w zakresie ochrony danych osobowych cz. 5 - instrukcja zarządzania systemem informatycznym	<ul style="list-style-type: none">- instrukcja jako dokument- polityka kluczy, ewidencja dostępu do pomieszczeń- plan ciągłości działania- regulamin użytkownika komputerów przenośnych i komórek- procedura niszczenia nośników danych oraz napraw w serwisach zewnętrznych- arkusz oceny ryzyka - przykład
15.45 – 16.00	Przerwa	
16.00 - 16.45	Dokumentacja w zakresie ochrony danych osobowych cz. 6 - inne dokumenty mające wpływ na ochronę danych osobowych	<ul style="list-style-type: none">- kodeksy dobrych praktyk- certyfikacje- regulaminy (pracy, wynagradzania, ZFŚS)- zalecenia organów nadzorczych/kontrolnych (np. rekomendacja D Komisji Nadzoru Finansowego, CSIZ, UODO)
16.45	ZAKOŃCZENIE	

DZIEŃ IV - Zgodność stosowanych praktyk z zasadami ochrony danych osobowych w obszarze kadrowym

10.00	OTWARCIE
10.00 – 10.30	<p style="text-align: center;">System ochrony danych osobowych w działach kadr. Czy tylko RODO?</p> <ul style="list-style-type: none"> - europejski system ochrony danych osobowych - system ochrony danych osobowych w Polsce - kodeks pracy, ustawy „zusowskie” oraz wydane na ich podstawie rozporządzenia i ich rola w ochronie danych osobowych, - jawność życia publicznego a ochrona danych osobowych - wpływ RODO na funkcjonowanie działów kadr
10.30 – 11.15	<p style="text-align: center;">Ochrona danych osobowych w procesach rekrutacyjnych</p> <ul style="list-style-type: none"> - poprawne klauzule z zakresu ochrony danych osobowych, jakie musi złożyć każdy kandydat w dokumentach aplikacyjnych - obowiązki informacyjne jakie należy spełnić wobec kandydatów do pracy – moment spełnienia obowiązków oraz przykładowe ich treści - zlecenie obsługi procesów rekrutacyjnych na zewnątrz – na co Dział Kadr musi zwrócić uwagę przy zawieraniu umów z agencjami rekrutacyjnymi, headhunterami, agencjami doradztwa personalnego? - przechowywanie danych osobowych kandydatów do pracy – jak długo można przechowywać aplikacje kandydatów? Od czego to zależy?
11.15 - 11.30	Przerwa
11.30 - 12.15	<p style="text-align: center;">Ochrona danych osobowych w procesach rekrutacyjnych c.d.</p> <ul style="list-style-type: none"> - jakich danych pracodawca nie może żądać od kandydata do pracy? - czy pracodawca może zbierać informacje o karalności kandydata do pracy? - czy poszukiwanie pracownika o nieposzlakowanej opinii oznacza możliwość uzyskania informacji o karalności? - czy pracodawca musi spełnić wobec kandydatów do pracy obowiązek informacyjny w zakresie przetwarzania ich danych osobowych? - dochodzenie roszczeń i ochrona praw jako element klauzuli informacyjnej i uzasadniony interes administratora danych osobowych - ochrona danych osobowych a umowa przedwstępna o pracę i list intencyjny, - czy pracodawca może przetwarzać dane zamieszczone przez kandydata w CV , jeśli wykraczają one poza zakres danych wskazanych przepisami
12.15 - 13.00	<p style="text-align: center;">Ochrona danych osobowych w procesach rekrutacyjnych c.d.</p> <ul style="list-style-type: none"> - czy pracodawca może przetwarzać dane szczególne umieszczone w CV kandydata do pracy? - czy i kiedy pracodawca może przetwarzać dane osobowe w różnych procesach rekrutacji? - czy i kiedy pracownik może skutecznie wycofać zgodę na przetwarzanie swoich danych osobowych? - rekrutacja on-line - na co warto zwrócić uwagę? - czy na gruncie RODO rekrutacje ukryte są dopuszczalne?? - obowiązki agencji zatrudnienia i pracodawcy w procesie rekrutacji prowadzonym wspólnie - RODO a rozmowa kwalifikacyjna - RODO a referencje
13.00 - 13.15	Obiad
13.15 - 14.00	<p style="text-align: center;">Ochrona danych osobowych w procesach rekrutacyjnych c.d.</p> <ul style="list-style-type: none"> - czy można zapytać uczelnię wyższą o jej absolwentów w toku rekrutacji? - dyskryminacja o RODO w rekrutacji - RODO w służbie cywilnej - otrzymywanie dokumentów rekrutacyjnych poza procesami rekrutacji, publikacja wyników rekrutacji, protokoły zniszczenia dokumentów - „czarna lista” pracowników a aktualne przepisy o ochronie danych osobowych - portal społecznościowy a złożenie oferty o pracę przez pracodawcę, weryfikacja pracownika na portalu społecznościowym w świetle RODO
14.00 - 15.00	<p style="text-align: center;">Ochrona danych osobowych w procesach kadrowych</p> <ul style="list-style-type: none"> - stare akta osobowe - nowe RODO – jak zapewnić zgodność w dokumentach kadrowych - kopia dowodu osobistego pracownika? - stan rodzinny pracownika a RODO - obowiązek informacyjny wobec pracownika, lista obecności, - wizerunek pracownika a inne dane osobowe pracownicze. - udostępnianie danych pracowników podmiotom zewnętrznym - kontakty ze związkami zawodowymi, z przychodniami medycyny pracy, szkolenia, delegacje, benefity pracownicze (ubezpieczenia grupowe, abonamenty sportowe i medyczne), - przekazywanie danych osobowych pracowników grupie kapitałowej, - monitoring poczty elektronicznej i wizyjny, GPS, - dane biometryczne, ewidencjonowanie czasu pracy przy użyciu nowoczesnych technologii
15.00 - 15.15	Przerwa
15.15 - 16.15	<p style="text-align: center;">Ochrona danych osobowych w procesach kadrowych</p> <ul style="list-style-type: none"> - Zakładowy Fundusz Świadczeń Socjalnych - zakres danych jakich można żądać od wnioskodawcy, konieczność pozyskania zgody, obowiązek informacyjny, okres przetwarzania danych osobowych, wytyczne dla członków komisji, okresowe przeglądy procesów przetwarzania danych osobowych - Praca na wybranych dokumentach z wykorzystaniem wzorców (wzór wniosku, wzór regulaminu, wzór klauzuli informacyjnej, wzór procedury rekrutacji, wzory oświadczeń pracowniczych, wzory zgód)
16.15 - 16.30	<p style="text-align: center;">Podsumowanie i zakończenie szkolenia</p> <ul style="list-style-type: none"> - Dyskusja z wykładowcami - Zasady udzielania porad ekspertów w ramach Forum Praktyków RODO - Możliwości dalszego poszerzania wiedzy w zakresie RODO
16.30	ZAKOŃCZENIE