1. **TYTUŁ:** Szkolenie z zakresu ochrony danych osobowych
2. **LICZBA GODZIN**: 24 godziny szkoleniowe x 7 edycji
3. **MIEJSCE REALIZACJI**: Chorzów ul. Składowa 17, sala 411 IVp.
4. **IMIĘ I NAZWISKO TRENERA:** Gołąb-Kobylińska Iwona
5. **FORMA ORGANIZACJI ZAJĘĆ:** Zajęcia prowadzone będą w grupach min. 20 do maks. 25-osobowych. Szkolenie dla każdej grupy zrealizowane zostanie w 3 dni. Godzina szkoleniowa to 45 minut. Dzień szkoleniowy obejmuje: dwie pięciominutowe, jedna dziesięciominutowa przerwa kawowa oraz jedna trzydziestominu-towa przerwa na lunch. Dominującą formą zajęć będą zajęcia warsztatowe.
6. **CEL: aktualizacja** wiedzy oraz umiejętności w zakresie ochrony danych osobowych.
7. **TEMATYKA ZAJĘĆ / LICZBA GODZIN**

Moduł	**Tematy zajęć**	**Liczba godzin**
Ochrona danych osobowych	1. Przegląd obowiązującego prawodawstwa. 2. Przegląd znowelizowanych ustaw. Co nowego w Kodeksie Pracy w kontekście RODO. 3. Definicje w pigułce – praca zdalna, dane osobowe, przetwarzanie, zbiory, usuwanie, anomimizacja, pseudonimizacja, ….. 4. Według jakich zasad przetwarzać dane osobowe: – zasada zgodności z prawem, rzetelności i przejrzystości, – zasada ograniczenia celu przetwarzania danych, – zasada minimalizacji danych, – zasada prawidłowości, – zasada ograniczenia przechowania danych, – zasada integralności i poufności danych, – zasada rozliczalności. 5. Jak określić podstawę prawną dla przetwarzanych danych osobowych. 6. Obowiązek informacyjny – jak skutecznie, kogo i o czym informować. 7. Zgody na przetwarzanie danych osobowych – kiedy są niezbędne, a kiedy niepożądane. 8. Zatrudnienie – co pracownik i kandydat wiedzieć powinien. 9. Prawa osób których dane przetwarzamy – jak je realizować. 10. Upoważnienia – jak prawidłowo upoważnić do przetwarzania danych osobowych i jak zarządzać uprawnieniami. 11. Inspektor Ochrony Danych – dla kogo obowiązek, dla kogo przywilej. 12. Umowy powierzenia przetwarzania danych osobowych – kiedy są niezbędne. 13. Rejestry – które musi, a które powinien prowadzić ADO. 14. Środki techniczne i organizacyjne – co zawiera polityka ochrony danych. 15. Instrukcja zarządzania systemami informatycznymi reliktem „starej” ustawy? 16. Zasada retencji – dlaczego jest tak ważna i jak ją ustalić.	10

	17. Naruszenia – czym są, kiedy, jak i do kogo je zgłaszać. 18. Szacowanie ryzyka – jak przeprowadzić i co zinwentaryzować. 19. Naruszenia ochrony danych osobowych – procedury reagowania. 20. Praca zdalna wyzwania i nowa rzeczywistość. a) Organizacja stanowisk pracy – co należy zabezpieczyć, a co i jak udostępnić, jak się porozumiewać i zadbać o bezpieczeństwo danych; b) Określenie modelu zarządzania informacją – co to są ścieżki obiegu dokumentów i transparentność hierarchii decyzyjnej oraz zasady dostępu do informacji; c) Procedury reakcji na zmiany otoczenia zewnętrznego – jak stosować monitoring i określić łańcuchy dystrybucji wygenerowanych decyzji; d) Delegowanie zadań operacyjnych i terminowych – tryby postępowania, czasookresy, plany awaryjne, motywacja pracownicza; e) Harmonogram pracy – godziny kontaktów, terminy wykonywania zadań i monitorowania poczty, social media; f) Komunikaty dla Odbiorców, Dostawców i Klientów – mechanizmy wymiany danych i ustalenia sposobu dystrybucji dokumentów; g) Zapewnienie efektywności pracy – praca w domu wyzwaniem dla wszystkich domowników, zakresy kontroli jakości pracy. 21. Aktualnie orzecznictwo. 22. Case study.	
RODO w kontekście sygnalisty	1. Regulacje prawne ochrony sygnalistów – zakres przedmiotowy i podmiotowy. a) Ochrona sygnalistów na gruncie prawa polskiego i unijnego; b) Rola i cel ochrony sygnalistów – założenia twórców regulacji; c) Podmioty prawne objęte ustawą o sygnalistach; d) Wyłączenia z mocy ustawy; e) Terminy wdrożenia nowych regulacji; f) Naruszenie prawa i ujawnianie nadużyć – co? gdzie? kiedy? g) Czy można wewnętrznie ograniczyć zakres dokonywanych zgłoszeń? h) Sankcje. 2. Sygnalista – podstawowe pojęcia. a) Definicja sygnalisty – kto może nim zostać; b) Warunki objęcia ustawą o ochronie sygnalisty; c) „Samodonos” – czy jest skuteczny? d) Zatrudnianie sygnalisty – czy można odmówić? e) Kiedy sygnalista traci ochronę; f) Sygnalista chroniony – a jego bliscy i znajomi? g) Odpowiedzialność sygnalisty – administracyjna, cywilna, karna, dyscyplinarna; h) Kiedy wyłącza się odpowiedzialność sygnalisty. 3. Kanały komunikacyjne – poufność, dostępność, ochrona przed ujawnieniem. a) Zgłoszenia wewnętrzne; b) Obowiązek raportowania; c) Zgłoszenia zewnętrzne – komu? I dlaczego? d) Ujawnienie publiczne – ostateczność? e) Formy zgłoszenia; f) Komunikacja z sygnalistą – czy zawsze jest możliwa? g) Zgłoszenia anonimowe – następstwa. 4. Procedura ochrony danych sygnalisty. a) Obligatoryjne elementy procedury zgodnie z ustawą; b) Opcjonalne elementy procedury;	4

	c) Konsultacja procedury ze stroną społeczną – kto? z kim? czy każdy? jak długo? d) Szkolenia, informowanie, powiadamianie – jak ogłosić jak zgłaszać? 5. Działania odwetowe. a) Rodzaje działań odwetowych; b) Środki ochrony sygnalistów. 6. Działania następcze. a) Poufność zgłoszeń; b) Czynności w ramach działań następczych; c) Weryfikacja zgłoszeń; d) Informacja zwrotna – nie zawsze możliwa; e) Bezstronność weryfikacji zgłoszenia. 7. Ochrona danych osobowych w procesie obsługi zgłoszeń przez sygnalistę. a) Zakres zmian koniecznych do przeprowadzenia w związku z wdrożeniem przepisów o ochronie sygnalistów; b) Umocowania osób przyjmujących zgłoszenia – osoba, stanowisko czy podmiot? c) Upoważnienia, zakresy obowiązków, niezależność; d) Klauzula informacyjna – co uwzględnić dodatkowo; e) Cel i zakres przetwarzania; f) Podstawa prawna przetwarzania danych osobowych; g) Co z ryzykiem przetwarzania danych? h) Retencja danych osobowych.	
RODO w kontekście dostępu do informacji publicznej	1. Informacja publiczna – regulacje prawne. a) Informacja publiczna – omówienie najważniejszych zasad wynikających z ustawy; b) Obowiązek czy dobrowolność udostępniania informacji publicznej? c) Prawo obywatela do dostępu do informacji publicznej - rola i znaczenie Biuletynu Informacji Publicznej; d) Prowadzenie Biuletynu Informacji Publicznej – zakres podmiotowy. 2. Redagowanie treści w Biuletynie Informacji Publicznej. a) Obligatoryjność i fakultatywność umieszczania poszczególnych informacji na stronie Biuletynu Informacji Publicznej? b) Informacje chronione przed udostępnieniem na witrynie Biuletynu Informacji Publicznej; c) Retencja danych – kryteria uwzględniane przy określaniu okresu przetwarzania dla danych umieszczonych w BIP; d) Jak prawidłowo oznaczyć informacje w BIP (wytworzył, udostępnił itp.)? e) Kto może być redaktorem BIP-u? – obligatoryjne i fakultatywne informacje o redakcji BIP; f) Aspekty techniczne BIP; g) Niepełnosprawni z dostępem do Biuletynu Informacji Publicznej. 3. Udostępnianie informacji publicznej na stronach BIP. a) Ustalenie osób pełniących funkcje publiczne; b) Zasady odnoszące do prywatności osób fizycznych których dane są publikowane – dopuszczalność przetwarzania danych osobowych; c) Tajemnice ustawowo chronione, prywatność, tajemnica przedsiębiorcy; d) Anonimizacja informacji zamieszczanych na witrynie BIP; e) Odpowiedzialność za nieudostępnienie informacji publicznej. 4. Dobre praktyki i sposoby unikania błędów przy redakcji BIP.	4

	a) Najczęstsze błędy popełniane przy redagowaniu Biuletynu Informacji Publicznej; b) Terminy na udostępnianie informacji publicznej za pośrednictwem BIP; c) Omówienie BIP-u na wybranych przykładach.	
Ochrona informacji niejawnych	1. Regulacje prawne. 2. Zakres przedmiotowy i podmiotowy ustawy o ochronie informacji niejawnych. 3. Organy odpowiedzialne za ochronę informacji niejawnych. 4. Organizacja i funkcjonowanie kancelarii tajnych i niejawnych. 5. Podstawowe zasady ochrony informacji niejawnych. 6. Zasady ochrony informacji niejawnej w systemie informatycznym. 7. Środki bezpieczeństwa fizycznego. 8. Bezpieczeństwo systemów teleinformatycznych. 9. Metody ochrony systemów teleinformatycznych. 10. Bezpieczeństwo osobowe. 11. Zagrożenia dla informacji. 12. Wymagana dokumentacja. 13. Prawo dostępu do informacji niejawnych. 14. Rola Agencji Bezpieczeństwa Wewnętrznego i Służby Kontrwywiadu Wojskowego.	4
RODO w pytaniach i odpowiedziach	1. Aktualne działania podejmowane przez Prezesa Urzędu Ochrony Danych Osobowych. 2. Rozwiązywanie problemów zgłaszanych przez uczestników. 3. Case study.	2
Razem		**24**