ENSI
KANCELARIA EKSPERTÓW

NAJBARDZIEJ DOŚWIADCZONY W POLSCE ZESPÓŁ EKSPERTÓW BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW INFORMATYCZNYCH

WARSZTATY EKSPERCKIE
SZACOWANIE RYZYKA ZGODNIE Z RODO I PRZEPROWADZENIE OCENY SKUTKÓW DLA OCHRONY DANYCH ZGODNIE Z NORMĄ ISO/IEC 29134

Szanowni Państwo,

Zapraszamy do udziału w wyjątkowych warsztatach eksperckich, które powstały **w oparciu o doświadczenie** zdobyte podczas pierwszego roku obowiązywania i stosowania 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 (RODO).

Warsztaty skierowane są do inspektorów ochrony danych oraz osób lub zespołów zajmujących się ochroną danych w organizacji.

Uczestnicy warsztatów otrzymają wyjaśnienie najważniejszych pojęć związanych z tematem warsztatów, a także wezmą udział w praktycznych ćwiczeniach szacowania ryzyka.

Podczas warsztatów, nasi **eksperci – praktycy** podzielą się z Państwem **wiedzą ekspercką** popartą **doświadczeniem** z zakresu stosowania RODO w obszarze szacowania ryzyka i oceny skutków. Udział w warsztatach zagwarantuje Państwu otrzymanie najważniejszych, rzetelnych informacji oraz praktycznego podejścia do tematu.

Nieliczne grupy uczestników podczas warsztatów, gwarantują skuteczną naukę oraz swobodną wymianę doświadczeń, jak również merytoryczne i przydatne dyskusje.

Program Warsztatów został opracowany przez Zespół Kancelarii Ekspertów ENSI, pod kierunkiem Prezesa ENSI p. **Macieja Byczkowskiego**, który brał udział w pracach sejmowych nad dwiema nowelizacjami ustawy o ochronie danych osobowych (2010 oraz 2014) oraz uczestniczy w pracach Grupy ds. Ochrony Danych Osobowych, powołanej przez Ministra Cyfryzacji.

Nasze warsztaty prowadzone są przez **specjalistów – praktyków** posiadających co najmniej 20-letnie doświadczeniem w przygotowywaniu organizacji do wypełnienia wymogów ustawy o ochronie danych osobowych, w przygotowaniu organizacji do wdrożenia RODO (od momentu wejścia Rozporządzenia w życie), a także w prowadzeniu szkoleń z zakresu ochrony danych osobowych. Prowadzący uczestniczą lub uczestniczyli w projektach wdrożenia RODO w ponad 100 organizacjach w Polsce. Pełnią także, w ramach outsourcingu, funkcję IOD w podmiotach różnych branż w Polsce.

Więcej informacji na temat prowadzących znajduje się na stronie https://csiod.ensi.net/prelegenci.html.
Zapraszamy!

Wszelkich informacji na temat warsztatów udziela **p. Aleksandra Jarzębska**:
tel.(22) 620 96 95 lub 620 12 00, e-mail: aleksandra.jarzebska_@_ensi.net, https://www.ensi.net

AGENDA WARSZTATÓW

I dzień	
9.30 – 13.30 (przerwa na kawę ok. 11.30 - 11.45)	**1. Szacowanie ryzyka i ocena skutków wg RODO:** a) Wymagania RODO w zakresie szacowania ryzyka - art. 24, 25, 32 b) Dobór odpowiednich zabezpieczeń dotyczący ochrony danych osobowych c) Wymagania RODO w zakresie oceny skutków dla ochrony danych (DPIA) – art. 35 d) Przykłady metodyk: o Normy ISO: 27005 oraz 29134 o Metodyka francuskiego organu nadzoru (CNIL) o Metodyka brytyjskiego organu nadzoru (ICO) e) Ogólne schematy postępowania: o Szacowanie ryzyka - schemat postępowania wg PN- ISO/IEC 27005 o DPIA – schemat postępowania wg wytycznych GR 29 (WP 248 rev.1) **2. Analiza ryzyka bezpieczeństwa informacji na bazie normy PN-ISO/IEC 27005:** a) Pojęcia podstawowe b) Proces zarzadzania ryzkiem c) Schemat postępowania d) Metody analizy ryzyka e) Postępowanie z ryzykiem f) Dokumentowanie zarządzania ryzykiem **3. Szacowanie ryzyka zgodnie z RODO dla wybranego procesu przetwarzania danych osobowych - ćwiczenia:** a) Ćwiczenie 1: Określanie kontekstu b) Ćwiczenie 2: Wykonanie szacowania ryzyka: o Zidentyfikowanie aktywów – zasobów danych osobowych o Zidentyfikowanie zagrożeń dla aktywów o Zidentyfikowanie istniejących zabezpieczeń o Zidentyfikowanie podatności o Zidentyfikowanie następstw (skutki dla osoby fizycznej oraz dla ADO)
13.30 – 14.30	Obiad
14.30-17.00	**4. Szacowanie ryzyka zgodnie z RODO dla wybranego procesu przetwarzania danych osobowych – ćwiczenia (cd):** a) Ćwiczenie 3: Wykonanie analizy ryzyka o Oszacowanie następstw o Oszacowanie prawdopodobieństwa incydentu o Określenie poziomu ryzyka b) Ćwiczenie 4: Ocena ryzyka i ustalenie planu postępowania z ryzykiem
II dzień	
9.30 – 13.30 (przerwa na kawę ok. 11.30 - 11.45)	**1. Ocena skutków dla ochrony danych (DPIA) zgodnie z wymaganiami RODO:** a) Konieczność przeprowadzenia DPIA (art. 35 i motyw 84 RODO) **2. Ocena skutków wg normy PN-ISO/IEC 29134:2018:** a) Różnica pomiędzy pojęciami PIA (*Privacy Impact Assessment*) a DPIA (*Data Protection Impact Assessment*) b) Ustalenie konieczności wykonania PIA c) Przygotowania do PIA o opisanie przedmiotu PIA o działania organizacyjne o planowanie zadań d) Wykonanie PIA: o identyfikacja przepływów danych

	o ustalenie wymogów w zakresie ochrony prywatności o szacowanie ryzyka dla prywatności o przygotowanie planu postępowania z ryzykami dla prywatności e) Działania po PIA **3. Zasady prywatności wg normy ISO/IEC 29100 w odniesieniu do wykonywania DPIA:** a) Ramy prywatności zgodnie z normą i ich niezbędność przy ocenie skutków dla ochrony danych zgodnie z RODO b) Pryncypia prywatności wg normy i ich odniesienie do wymogów RODO **4. Ocena skutków dla ochrony danych zgodnie z RODO dla wybranego procesu przetwarzania danych osobowych - ćwiczenia:** a) Ćwiczenie 1: Określenie konieczności wykonania DPIA b) Ćwiczenie 2: Identyfikacja Interesariuszy, określenie potrzeb w zakresie konsultacji i sporządzenie ich planu c) Ćwiczenie 3: Opisanie zakresu oceny o Określenie kontekstu o Opis planowanego sposobu realizacji praw podmiotów danych o Identyfikacja i opis aktywów wspierających przetwarzanie danych osobowych d) Ćwiczenie 4: Opracowanie diagramu przepływu danych osobowych
13.30 – 14.30	Obiad
14.30 – 17.00	**5. Ocena skutków dla ochrony danych zgodnie z RODO dla wybranego procesu przetwarzania danych osobowych – ćwiczenia (cd):** a) Ćwiczenie 5: Ustalenie istotnych wymogów w zakresie ochrony prywatności i ocena zgodności (odniesienie do pryncypiów prywatności w kontekście wymogów RODO) b) Ćwiczenie 6: Szacowanie ryzyka dla prywatności o Identyfikacja ryzyk o Analiza ryzyka o Ocena ryzyka – sporządzenie mapy ryzyka o Wybór opcji postępowania z ryzykiem oraz dobór mechanizmów kontroli o Opracowanie planu postępowania z ryzykami c) Ćwiczenie 7: Opracowanie raportu z DPIA
17.00	**Zakończenie warsztatów i rozdanie dyplomów**

Prowadzący: Maciej Byczkowski (Prezes Zarządu ENSI – szef Zespołu Kancelarii Ekspertów ENSI),
Piotr Wojakowski (Dyrektor ds. bezpieczeństwa ENSI)

Maciej Byczkowski

Prezes Zarządu ENSI, od 2007 r. Prezes Zarządu SABI - Stowarzyszenia Inspektorów Ochrony Danych (wcześniej: Stowarzyszenia Administratorów Bezpieczeństwa Informacji). Pełnił funkcję Członka Zarządu Związku Firm Ochrony Danych Osobowych - ZFODO (2018-2019). Pełnił funkcję wiceprzewodniczącego Komitetu Bezpieczeństwa Biznesu Krajowej Izby Gospodarczej (2004 - 2013). Brał udział w pracach: sejmowej Komisji Sprawiedliwości i Praw Człowieka nad nowelizacją ustawy o ochronie danych osobowych (2007 - 2010); pracach Zespołu ekspertów powołanego przez GIODO, który opracował projekt zmiany ustawy o ochronie danych osobowych w ramach ustawy deregulacyjnej Ministerstwa Gospodarki dla przedsiębiorców (2011 - 2014); sejmowej Komisji Nadzwyczajnej ds. związanych z ograniczeniem biurokracji nad nowelizacją ustawy o ochronie danych osobowych w ramach ustawy o ułatwieniu wykonywania działalności gospodarczej - deregulacja IV (2014) oraz pracach Ministerstwa Administracji i Cyfryzacji nad opracowywaniem nowych projektów wykonawczych do ustawy o ochronie danych osobowych w zakresie wykonywania zadań ABI (2014 - 2015). Uczestniczył również w pracach nad zmianą rozporządzenia wykonawczego w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i

organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych do ustawy o ochronie danych osobowych oraz konsultacjach w przygotowaniu polskiego stanowiska na forum Rady Europy w związku z reformą ochrony danych osobowych w Unii Europejskiej. Ekspert i audytor bezpieczeństwa informacji i systemów informatycznych (ponad 20 lat doświadczeń). Współtwórca Metodyki TISM, Metodyki TSM-BCP, Metodyki TSM - całościowej koncepcji zarządzania bezpieczeństwem w organizacji. Twórca metodyki Zarządzania Procesami Przetwarzania Danych Osobowych (PBDO). Wraz z zespołem przygotował ponad 400 organizacji do wypełniania wymogów ustawy o ochronie danych osobowych; przeszkolił ponad 30 000 osób. Pełnił od 1999 r. funkcję ABI – a obecnie od 25 maja 2018 r. pełni funkcję Inspektora Ochrony Danych (w ramach outsourcingu) w różnych organizacjach. Prowadził wiele projektów wdrożeń Polityki Bezpieczeństwa Informacji (wg TISM oraz normy ISO 27001) w organizacjach wielu branż w Polsce. Absolwent Politechniki Warszawskiej. Wykładał na Politechnice Warszawskiej (Wydział Zarządzania) - Studium podyplomowe "Zarządzanie Jakością i Bezpieczeństwem Informacji w środowisku IT" oraz na Akademii im. Leona Koźmińskiego w Warszawie - Studia podyplomowe "Ochrona Danych Osobowych i Informacji Niejawnych". Aktualnie wykłada w Polskiej Akademii Nauk na Studiach podyplomowych "Wykonywanie funkcji inspektora ochrony danych" (w ramach którego jest również członkiem Rady Programowej). Autor licznych publikacji z dziedziny bezpieczeństwa informacji i systemów informatycznych oraz ochrony danych osobowych. Uczestniczy lub uczestniczył w projektach wdrożenia RODO w ponad 100 organizacjach w Polsce. Brał udział w pracach Grupy ds. Ochrony Danych Osobowych, powołanej przez Ministra Cyfryzacji.

Piotr Wojakowski

Dyrektor ds. bezpieczeństwa w ENSI Sp. z o.o. Ekspert ENSI w dziedzinie zarządzania bezpieczeństwem systemów informatycznych, zarządzania bezpieczeństwem informacji oraz szacowania ryzyka związanego z bezpieczeństwem informacji. Związany z firmą od 1999 r. (wcześniej na stanowiskach: audytor bezpieczeństwa systemów informatycznych, kierownik zespołu testów penetracyjnych). Absolwent Politechniki Warszawskiej Wydziału MEiL. Współtwórca: metodyki testów i audytów systemów informatycznych ENSI, metodyki TISM - zarządzania bezpieczeństwem informacji w organizacji, metodyki TSM-BCP - zarządzania ciągłością działania biznesowego. Wykładowca Politechniki Warszawskiej - Studium Podyplomowego "Zarządzanie Jakością i Bezpieczeństwem Informacji w środowisku IT" oraz na Polskiej Akademii Nauk - Studia podyplomowe "Wykonywanie funkcji Administratora bezpieczeństwa informacji i inspektora ochrony danych". Posiada wieloletnie doświadczenie we wdrażaniu i audytowaniu zabezpieczeń systemów informatycznych, testowaniu bezpieczeństwa aplikacji internetowych, kierowaniu projektami wdrożeń Polityki Bezpieczeństwa Informacji, opracowywaniu i wdrażaniu procedur bezpieczeństwa dotyczących zarządzania systemami informatycznymi, szacowania ryzyka dotyczącego bezpieczeństwa informacji oraz przygotowywania planów zachowania ciągłości działania w przedsiębiorstwach sektora bankowo-finansowego, przemysłowego oraz w przedsiębiorstwach o szczególnym znaczeniu gospodarczo-obronnym, szkoleniu kadry menedżerskiej z zasad ochrony informacji (ponad 700 osób przeszkolonych na otwartych i zamkniętych Warsztatach TISM). Brał lub bierze udział w kilkudziesięciu projektach przygotowujących różne organizację do wdrożenia RODO. Ponadto od 2004 r. pełnił funkcję zastępcy ABI w różnych spółkach. Obecnie jest w zespole eksperckim wspierającym Inspektora ochrony danych. Posiada następujące certyfikaty: Certified Information Systems Security Professional (Certificate No: 62105), Certyfikowany audytor wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji wg BS 7799-2:2002, Certyfikowany audytor wiodący ISO 27001:2005 (Cert No: Ex 114: 06192), Certyfikowany inżynier systemu BorderWare Firewall Server, Certyfikowany administrator systemów Checkpoint FirewalI (Check Point Certified Professional ID: 445960310 CCSA 2000), MicrosoftR Certified Technology Specialist