

## Praktyczna ochrona danych osobowych w jednostkach samorządu terytorialnego

Na całym świecie gwałtownie wzrasta liczba i skala incydentów bezpieczeństwa w systemach informatycznych. Ocenia się, że ataki hakerów kosztują świat 500 mld \$ rocznie. Aby zapobiec tym incydentom państwa wprowadzają coraz bardziej restrykcyjne wymagania dotyczące ochrony danych osobowych. Powoduje to, że wszelkie organizacje działające z danymi osobowymi, w coraz to łatwiejszy sposób mogą narazić się na naruszenie lub nadużycie przepisów, co może się wiązać z dużym ryzykiem dla samej organizacji. W dzisiejszych czasach prawo wymaga od jednostek samorządu terytorialnego chronienia danych osobowych swoich interesariuszy. Jednostki które prawidłowo chronią dane osobowe, nie tylko zapobiegają nałożeniu na siebie kar, ale również zwiększają zaufanie interesantów. Dokumentacja bezpieczeństwa jest wymagana przez prawo, ale nie będzie ona działać prawidłowo, jeśli będzie po prostu narzucona. Taka dokumentacja staje się bezużyteczna, a działania administratora danych zostaną ocenione negatywnie. Liczy się zrozumienie obowiązujących przepisów oraz odpowiednia świadomość, że zapewnienie bezpieczeństwa informacji to proces, który wymaga ciągłego udoskonalenia. Utrata poufności danych to ryzyko utraty wizerunku (czasami już nie do odzyskania) i ryzyko prawne (kary określone w przepisach).

W połowie maja 2018r. wejdą w życie nowe regulacje dotyczące ochrony danych osobowych RODO. Nowe rozporządzenie zmienia wiele dotychczasowych wymagań i obliuguje organy zarządzające danymi do zmiany dotychczasowego podejścia. Wprowadzenie w życie nowych wymagań może być dla wielu organizacji problemem, szczególnie jeśli powiążemy wymagania RODO z wymaganiami dotyczącymi ogólnie pojętego bezpieczeństwa informacji. Jedną z metod umożliwiających spełnienie nowych wymagań jest wdrożenie elementów systemu zarządzania bezpieczeństwem informacji opartego o wymagania normy ISO 27001. Organizacja pracująca zgodnie z normą, w sposób o wiele prostszy jest w stanie dostosować się do nowych wymagań oraz ma prawo do zwolnienia z pewnych wymagań RODO, takich jak przeprowadzanie audytów bezpieczeństwa (zgodnie z Krajowymi Ramami Interoperacyjności, minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnymi wymaganiami dla systemów teleinformatycznych).

Zapraszamy Państwa na szkolenie, którego celem jest wspólne omówienie normy ISO 27001 i przedstawienie jej w nowym świetle oraz zapoznanie się z nowym rozporządzeniem RODO. Wspólnie prześledzimy wymagania, na tle tego jak funkcjonuje urząd i jak zapewnia ochronę danych osobowych. Chcemy otworzyć nieprzekonanym oczy na ochronę danych osobowych, a przekonanym pokazać nowe narzędzia do lepszego zarządzania nią.



### **Agenda szkolenia jest następująca:**

godz. 9:00-10:30 - szkolenie  
godz. 10:30-10:45 - przerwa kawowa  
godz. 10:45-12:15 - szkolenie  
godz. 12:15-12:45 – przerwa kawowa  
godz. 12:45-14:15 - szkolenie  
godz. 14:15-14:30 - przerwa kawowa  
godz. 14:30- 16:00 - szkolenie.



### **Program szkolenia obejmuje:**

1. Wstęp do normy ISO 27001 w kontekście interoperacyjności
2. Przegląd wymagań ISO 27001 (Deklaracja stosowania, analiza ryzyka, plany działań)
3. Wstęp do RODO
4. Przegląd wymagań RODO
5. Korzyści płynące z wdrożenia ISO 27001 w kontekście wymagań RODO

### **Metody wykorzystywane na szkoleniu:**

- ▶ Prezentacja multimedialna,
- ▶ Dyskusja w grupie,
- ▶ Warsztaty.

### **Trener:**

Piotr Maćkowiak – Konsultant i audytor w zakresie systemów zarządzania w tym ISO 9001 i ISO 27001, przeprowadził ponad 100 szkoleń w ramach projektów realizowanych dla JST, ochroną danych osobowych zajmuje się od 2014 roku, nieprzerwanie od 2015 pełni funkcję ABI, członek stowarzyszenia ABI, w 2016 ukończył studia podyplomowe Administrator Bezpieczeństwa Informacji (WSB), absolwent Politechniki Poznańskiej – kierunek: mechatronika

**Koszt szkolenia:**

300,00 złotych netto od osoby.

Koszt obejmuje materiały szkoleniowe oraz przerwy kawowe.

**Zgłoszenia:**

Zgłoszenie należy przesłać do dnia 20 września 2017 roku. Skan zgłoszeni prosimy przesłać mailem na adres: [szkolenia@dgpmc.pl](mailto:szkolenia@dgpmc.pl).

**Miejsce szkolenia:**

Szkolenie odbędzie się w dniu 26 września 2017 roku w Poznańskim Parku Technologiczno-Przemysłowym (sala C) przy ul. 28 Czerwca 1956 r. 400 w Poznaniu (2 minuty drogi od węzła autostradowego Poznań Dębiec).

