- **Szkolenie z zakresu ochrony danych osobowych w Polskim Towarzystwie Ekspertów Dochodzeń Popożarowych –**

I. Najważniejsze informacje na temat RODO:

RODO - Jest to unijne rozporządzenie dotyczące ochrony każdej osoby fizycznej, w związku z przetwarzaniem danych osobowych i w sprawie ich swobodnego przepływu. Od 25.05.2018 r. wraz z nową ustawą o ochronie danych osobowych, tworzy nowy porządek prawny w naszym kraju.

1. Wyznaczenie inspektora ochrony danych (art. 37-39 RODO)
Inspektor ochrony danych IOD jest odpowiednikiem dawnego administratora bezpieczeństwa informacji. Od 25 maja, niektóre podmioty będą zmuszone zatrudnić osobę pełniącą funkcję IOD. Rozporządzenie o ochronie danych osobowych w art. 37 jasno precyzuje sytuacje, kiedy administrator danych osobowych będzie musiał wyznaczyć inspektora. W przypadku PTEDP nie został wyznaczony IOD.

2. Obowiązek informacyjny (art. 12-14 RODO)
Unijne rozporządzenie rozszerza katalog informacji, jakie administratorzy danych osobowych będą musieli udostępnić osobom, których dane pobierają i przetwarzają. Rozporządzenie nakazuje, aby obowiązek został przedstawiony w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie. Ważne, żeby został napisany jasnym i prostym językiem, szczególnie jeśli informacje kierowane są do dziecka. Osoba, której dane dotyczą będzie miała prawo uzyskać informacje na temat przetwarzania jej danych. Administrator danych będzie zobowiązany, bez zbędnej zwłoki, najpóźniej w ciągu miesiąca, odpowiedzieć wnioskodawcy.

3. Nowe prawa obywateli (art. 15-21 RODO)
Rozporządzenie o ochronie danych osobowych przyznaje osobom, których dane są przetwarzane rozszerzone uprawnienia.
Prawa osób, których dane dotyczą:

- prawo dostępu przysługujące osobie, której dane dotyczą,
- prawo do sprostowania danych,
- prawo do usunięcia danych („prawo do bycia zapomnianym”),
- prawo do ograniczenia przetwarzania,
- prawo do przenoszenia danych,
- prawo do sprzeciwu.

Na szczególną uwagę zasługuje prawo do bycia zapomnianym, które nakłada na administratora obowiązek usunięcia danych osobowych w całości z jego systemu. W przypadku Internetu, oznacza to, że usunięte muszą zostać również wszelkie linki, kopie i repliki danych, nawet jeśli są one w posiadaniu innych podmiotów przetwarzających te dane w jego imieniu.

4. Rejestrowanie czynności przetwarzania (art. 30 RODO)
Administrator danych osobowych ma obowiązek prowadzić rejestr czynności przetwarzania. Natomiast w przypadku procesorów, istnieje konieczność prowadzenia rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu ADO.

Nowy obowiązek spoczywa na większości administratorów danych osobowych i podmiotów przetwarzających dane. Takie rejestry będą musiały prowadzić podmioty które:

- zatrudniają powyżej 250 pracowników,
- przetwarzają szczególne kategorie danych (dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby),
- przetwarzają dane w sposób, który narusza lub może naruszać prawa i wolności osób, których dane dotyczą,
- przetwarzają dane w sposób ciągły, czyli nie mają charakteru sporadycznego,
- przetwarzają wyroki skazujące lub informacje o naruszeniu przepisów prawa.

5. Zgoda (art. 7 RODO)

Administrator danych osobowych musi wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie danych osobowych. Rozporządzenie nakazuje, iż zgoda musi być wyrażona konkretnemu podmiotowi. Oświadczenie zgody musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii. Ważne, aby było przygotowane w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Osoba, której dane dotyczą, musi mieć zapewnione prawo do wycofania zgody w tak samo łatwy sposób, jak doszło do jej wyrażenia.

6. Ocena skutków dla ochrony danych (art. 35 RODO)

Kolejnym, nowym obowiązkiem spoczywającym na administratorze danych osobowych, które nakłada rozporządzenie o ochronie danych osobowych, jest przeprowadzenie oceny skutków dla ochrony danych (DPIA). RODO wymaga, aby przedsiębiorcy przetwarzający dane osobowe, przeprowadzili analizy wpływu działań na danych osobowych na ryzyko naruszenia praw osób, których dotyczą. Przeprowadzenie oceny będzie konieczne w dwóch przypadkach: stwierdzenia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych oraz kiedy zadecyduje o tym organ nadzorczy (Prezes Urzędu Ochrony Danych Osobowych).

7. Ograniczone profilowanie (art. 22 RODO)

Rozporządzenie reguluje zasady dotyczące zautomatyzowanego podejmowania decyzji. Głównie chodzi o profilowanie, które wg art. 4 pkt. 4 RODO oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych. Polega to na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej. Wykorzystywane w szczególności do analizy lub prognozy efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
Rozporządzenie o ochronie danych osobowych uwzględnia możliwość profilowania w 3 przypadkach: jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem, wynika z przepisów prawa, osoba, której dane dotyczą wyraziła na to zgodę.

8. Zgłoszenie naruszeń (art. 33 RODO)

Administrator danych będzie miał obowiązek zgłosić naruszenie ochrony danych osobowych do właściwego organu nadzorczego. Rozporządzenie o ochronie danych osobowych przewiduje na to 72 godziny od stwierdzenia naruszenia. Obowiązek nie

powstaje w przypadku, kiedy istnieje małe prawdopodobieństwo, że incydent skutkował ryzykiem naruszenia praw lub wolności osób fizycznych. W przeciwnym razie, ADO będzie musiał powiadomić nie tylko organ nadzorczy, ale również wszystkie osoby, których dane dotyczą. Administrator danych samodzielnie będzie musiał ocenić, czy naruszenie powinno zostać zgłoszone.

9. Kary za niewłaściwe przetwarzanie danych osobowych (art. 83 RODO)
Naruszenie przepisów o ochronie danych osobowych to straty wizerunkowe, ale również finansowe. Rozporządzenie o ochronie danych osobowych przewiduje kary nawet do 20 milionów euro bądź 4 proc. obrotu światowego w związku z wyciekiem bądź incydentem związanym z danymi osobowymi. Kary pieniężne w każdym przypadku mają być odstraszające, proporcjonalne i skuteczne. Będą zależały od charakteru, wagi i czasu trwania naruszenia oraz innych czynników takich jak np. próba zminimalizowania ryzyka.

II. Zasady przetwarzania danych osobowych w PTEDP

1. Przetwarzane dane osobowe powinny być pozyskiwane wyłącznie dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.
2. Przetwarzanie danych osobowych następuje wyłącznie na podstawie pisemnego upoważnienia podpisanego przez Administratora.
3. Przetwarzane dane osobowe powinny być merytorycznie poprawne i adekwatne w stosunku do celu, w jakim są przetwarzane. Zabrania się zbierania danych nieistotnych o większym stopniu szczegółowości niż jest to niezbędne do realizacji celu.
4. Dane mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dane dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celów przetwarzania.
5. Dane osobowe przetwarzane są zgodnie z „Rejestrem czynności przetwarzania” obowiązującego w PTEDP.
6. Przetwarzanie danych osobowych możliwe jest na podstawie zgody wyrażonej pisemnie przez osobę, której dane dotyczą i wobec której został wypełniony obowiązek informacyjny.
7. Obszarem przetwarzania danych osobowych jest siedziba PTEDP oraz nośniki papierowe i teleinformatyczne używane przez upoważnione osoby poza siedzibą.
8. Za bezpieczeństwo nośników odpowiada osoba z nich korzystająca. Niedopuszczalne jest pozostawienie nośników bez osobistego nadzoru. Nośniki teleinformatyczne muszą być zablokowane hasłem, a ich oprogramowanie zabezpieczone programem antywirusowym i na bieżąco aktualizowane. Należy pamiętać o cyklicznej zmianie hasła. Ustawienia monitora powinno uniemożliwić podgląd dokumentu osobom nieupoważnionym.
9. Przed przekazaniem sprzętu teleinformatycznego do serwisu należy usunąć z niego wszelkie dane osobowe, pozwalające na identyfikację danej osoby.
10. Nośniki papierowe z danymi osobowymi powinny być przechowywane w zamykanych na klucz szafach. Bezwzględnie obowiązuje zasada „czystego biurka”.

11. Niszczenie dokumentacji papierowej powinno przebiegać z gwarancją ich całkowitego zniszczenia.
12. W przypadku niezamierzonego wycieku danych osobowych, należy ten fakt niezwłocznie zgłosić Prezesowi PTEDP lub w przypadku jego nieobecności osobie go zastępującej.

III. Prezentacja na temat RODO – do celów szkoleniowych realizowanych przez Zarząd PTEDP.