Warszawa, dnia 9 kwietnia 2018 r.

Bezpieczeństwo danych – problemy prawne i techniczne

Przygotowania Zakładu Ubezpieczeń Społecznych do wypełniania obowiązków administratora wynikających z unijnego ogólnego rozporządzenia o ochronie danych (RODO)

Tomasz Chromiński

ZUS ZAKŁAD UBEZPIECZEŃ SPOŁECZNYCH

- ✓ W Zakładzie Ubezpieczeń Społecznych został opracowany i zatwierdzony przez Prezesa Zakładu - Plan realizacji zadań mających na celu przygotowanie do wypełniania obowiązków administratora wynikających z unijnego ogólnego rozporządzenia o ochronie danych – RODO.

- ✓ Równolegle, powołany został Zespół roboczy ds. koordynacji wdrożenia RODO. Zespół monitoruje postęp prac związanych z realizacją zadań określonych w Planie oraz podejmuje decyzje zmierzające do intensyfikacji działań.

- ✓ Zakład zawarł umowę z podmiotem zewnętrznym - kancelarią prawną. Umowa dotyczy wsparcia prawnego w przedmiotowym obszarze działań, w tym w szczególności formułowania kierunkowych opinii prawnych.

- ✓ Przeprowadzony został wewnętrzny audyt - jako zadanie doradcze w zakresie oceny stopnia i prawidłowości realizacji zadań mających na celu przygotowanie Zakładu do wejścia w życie przepisów RODO.

Dokonano szczegółowej analizy operacji przetwarzania danych osobowych wyszczególnionych w modelu zarządzania procesowego w ZUS, w wyniku czego zostały opracowane dokumenty stanowiące :

- wykaz kategorii osób, których dotyczą dane przetwarzane w Zakładzie Ubezpieczeń Społecznych,

- opis celów przetwarzania danych i podstawy prawne przetwarzania - w odniesieniu do poszczególnych kategorii osób oraz kategorii przetwarzanych danych.

Dokonano pełnej oceny czy przetwarzanie danych odbywa się zgodnie z zasadami, o których mowa w art. 5 RODO :

- zgodność z prawem, rzetelność i przejrzystość,
- ograniczenia celu przetwarzania,
- adekwatności danych do celów przetwarzania - minimalizacja danych,
- prawidłowość danych w świetle celów ich przetwarzania,
- ograniczenia przechowywania,
- integralności i poufności.

Do dnia 25 maja 2018 r. w Zakładzie zostanie sformułowany dokument, uzasadniający w sposób przejrzysty, że w organizacji są przestrzegane wymienione wyżej zasady – zasada rozliczalności

Przeprowadzono analizę przepisów RODO, w celu ustalenia:

- w jakim zakresie obowiązki i prawa wynikające z Rozporządzenia będą miały zastosowanie w odniesieniu do Zakładu,

- które z obowiązków Zakładu należałoby ograniczyć polskim aktem prawnym na podstawie art. 23 ust. 1 RODO.

W wyniku poczynionych ustaleń, Zakład skierował do Ministra Rodziny Pracy i Polityki Społecznej wystąpienie zawierające propozycję wraz z uzasadnieniem w zakresie wyłączeń przepisów RODO w odniesieniu do Zakładu - propozycja dotyczy wyłączenia stosowania przepisów art. 13 ust. 1 i 2 i art. 14 ust. 1 i 2 oraz art.18.

Zakład przetwarza dane osobowe ponad 16 mln ubezpieczonych i ok. 7 mln świadczeniobiorców oraz dane ok. 43 tys. pracowników zatrudnionych w ZUS. Każdorazowe przekazywanie osobom informacji określonych w przepisach RODO, byłoby połączone z niewspółmiernie dużym wysiłkiem, wysokim kosztem realizacji tych obowiązków oraz innymi potencjalnymi nakładami.

Na Zakładzie spoczywa jednakże obowiązek podjęcia „odpowiednich środków", które pozwolą mu na skuteczne wywiązanie się z obowiązku informacyjnego.

Mając na uwadze, że przepisy RODO nie wskazują sposobu, w jakim nastąpić ma przekazywanie przedmiotowych informacji, w celu realizacji obowiązków informacyjnych wymienionych w przepisach art. 13 ust. 1 i 2 i art. 14 ust. 1 i 2, przyjęto rozwiązanie zakładające zamieszczenie przedmiotowych informacji, na stronie podmiotowej ZUS (w Biuletynie Informacji Publicznej). Równoległym działaniem będzie dystrybucja tych niespersonalizowanych informacji z wykorzystaniem dostępnych kanałów w salach obsługi bezpośredniej klientów ZUS.

Art. 18 RODO – prawo do ograniczenia przetwarzania.

Zakład, jako państwowa jednostka organizacyjna działa na podstawie i w granicach prawa. Przetwarzane przez Zakład dane osobowe są niezbędne do ustalenia określonych praw i obowiązków osób ubezpieczonych i płatników składek, które wynikają bezpośrednio z wielu przepisów prawa.

Wyłączenie wobec ZUS obowiązku stosowania przepisu art. 18, mieści się w zakresie przesłanki określonej w art. 23 ust. 1 lit. e RODO tj. nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznych społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym celom określonym w tym przepisie.

W Zakładzie trwają prace związane z opracowaniem dokumentacji związanej z:

- ✓ określeniem zasad i sposobu zarządzania ryzykiem naruszenia praw i wolności osób fizycznych w związków z przetwarzaniem danych osobowych w Zakładzie.

- ✓ określeniem zasad i sposobu dokumentowania realizacji wymagań określonych w art. 33 i 34 RODO, w tym ;

- wykrywaniem naruszeń ochrony danych osobowych oraz ocenianiem prawdopodobieństwa naruszenia ochrony danych, które mogą skutkować naruszeniem praw i wolności osób fizycznych;
- zgłaszaniem naruszeń ochrony danych osobowych organowi nadzorczemu, a w wypadku gdy naruszenie ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych - zawiadamianiem osoby której dane dotyczą.

Zgodnie z art. 34 ust.3 zawiadomienie o naruszeniu które może powodować wysokie ryzyko naruszenia lub wolności osób fizycznych, nie jest wymagane, w przypadkach gdy:

- administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie,

- administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby,

- wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

- ✓ W Zakładzie został opracowany rejestr czynności przetwarzania danych osobowych zgodnie wymogami określonymi w art. 30 ust. 1 RODO. Dokument ten jest na bieżąco uzupełniany o wyniki ustaleń dokonywanych w ramach trwających prac związanych z przygotowaniem Zakładu do stosowania przepisów RODO.

- ✓ W związku z obowiązkiem wyznaczenia inspektora ochrony danych, zostały podjęte działania zmierzające do wprowadzenia zmian w strukturze organizacyjnej ZUS oraz zdefiniowania zasad funkcjonowania IOD w Zakładzie.

- ✓ W Zakładzie dokonywany jest aktualnie przegląd obowiązujących umów, pod kątem prawidłowości zapisów mówiących o powierzeniu przetwarzania danych osobowych oraz konieczności aneksowania tych umów, z uwzględnieniem sytuacji przetwarzania wymagających rozróżnienia między administratorem i podmiotem przetwarzającym.

- ✓ Prace prowadzone są w oparciu o wypracowane wzory jednolitych postanowień klauzul umownych, które uwzględniają wymogi wynikające z RODO w zakresie powierzenia przetwarzania danych osobowych, w szczególności określone w przepisach art. 24, 26 i 28 RODO.

- ✓ Dobiega końca proces ustalania, czy w organizacji odbywa się przetwarzanie danych osobowych na podstawie zgody osoby, której dane dotyczą - w rozumieniu art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO.

Uzyskanie zgody na przetwarzanie danych osobowych byłoby niezbędne do legalizacji działań wówczas, gdy nie możliwym będzie wskazanie przepisu prawa UE lub prawa krajowego, uprawniającego do przetwarzania danych osobowych.

Przedmiotowe ustalenie dokonywane jest z uwzględnieniem:

- kategorii osób, których takie przetwarzanie dotyczy,
- zakresu danych i celu przetwarzania danych,
- okresu przetwarzania i kryteriów ustalenia tego okresu.

Dziękuję za uwagę

ZAKŁAD
UBEZPIECZEŃ
SPOŁECZNYCH