Warszawa, 04.05.2021 r.

Obowiązki pracodawcy w zakresie ochrony danych osobowych, który wprowadził PPK dla swoich pracowników

Zgodnie z ustawą z dnia 4 października 2018 r. o pracowniczych planach kapitałowych każda organizacja, która zatrudnia co najmniej jedną osobę podlegającą obowiązkowo ubezpieczeniom emerytalnemu i rentowemu, musi otworzyć pracownicze plany kapitałowe (PPK) dla swoich pracowników i zleceniobiorców. PPK są prowadzone przez instytucję finansową na podstawie umowy o prowadzenie PPK, zawieranej przez pracodawcę w imieniu i na rzecz pracowników.

Bez wchodzenia w większe szczegóły można spokojnie stwierdzić, że zarówno pracodawca, jak i instytucja finansowa w kontekście PPK będą pełnić funkcję odrębnych administratorów danych.

W niniejszym artykule interesuje nas sytuacja pracodawcy, a zatem w kontekście PPK można wskazać następujące obowiązki po jego stronie:

1) konieczność aktualizacji (albo opracowania nowego) obowiązku informacyjnego wobec pracowników, którzy przystąpią do PPK,
2) konieczność aktualizacji rejestru czynności przetwarzania danych – w kontekście PPK pojawią nam się nowe czynności przetwarzania, a zatem musimy je odnotować w RCP,
3) konieczność implementacji mechanizmów związanych z przestrzeganiem okresów retencji danych przewidzianych dla danych potrzebnych dla celów PPK (niszczenie dokumentów, anonimizacja danych w systemach teleinformatycznych),
4) przeprowadzenie oceny ryzyka dla przetwarzania danych, a gdyby się okazało, że to ryzyko jest duże – sięgnięcie po DPIA.

Ad. 1
Jak może wyglądać przykładowy obowiązek informacyjny w zw. z PPK? Poniżej przykład:

Pracodawca, tj.: XYZ Sp. z o.o. („XYZ") informuje, że jest administratorem danych osobowych przetwarzanych w związku z prowadzonym programem pracowniczych planów kapitałowych (PPK). Kontakt z administratorem jest możliwy poprzez e-mail: bok@xyz.pl. Kontakt z powołanym w XYZ Inspektorem Ochrony Danych jest możliwy poprzez e-mail: iod@xyz.pl.

Poza przetwarzaniem danych osobowych pracowników w celach związanych z zatrudnieniem, o czym pracownik był odrębnie poinformowany, XYZ na potrzeby realizacji programu PPK przetwarza dane osobowe w celu wykonania obowiązków, o których mowa w ustawie o pracowniczych planach kapitałowych, a zatem na podstawie art. 6 ust. 1 lit. c 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 (dalej jako „RODO") w związku z przepisami ww. ustawy. W ramach realizacji tych obowiązków mieści się między innymi:

1) zawarcie i realizacja umowy o zarządzanie PPK z wybraną instytucją finansową,
2) zawarcie i realizacja umowy o prowadzenie PPK w imieniu i na rzecz osób zatrudnionych w XYZ z tą samą instytucją finansową,
3) przyjęcie składanej deklaracji przystąpienia do PPK bądź innych deklaracji dotyczących PPK, wymaganych wspomnianą ustawą, terminowe i prawidłowe obliczanie oraz przekazywanie wpłat do wybranej instytucji finansowej,
4) gromadzenie i archiwizacja dokumentacji dotyczącej PPK,

5) przekazywanie pracownikom oraz wybranej instytucji finansowej informacji związanych z utworzonymi PPK

Dane będą również przetwarzane w związku z dochodzeniem/obroną roszczeń oraz w celu wykazania realizacji obowiązków związanych z wprowadzeniem PPK, co stanowi uzasadniony interes XYZ (podstawa prawna przetwarzania danych wynika z art. 6 ust. 1 lit. f RODO). Archiwizacja dokumentów zawierających dane niezbędne do PPK następuje na podstawie przepisów ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (10 lat).

Realizacja obowiązków XYZ wynikających z ustawy o pracowniczych planach kapitałowych obejmuje udostępnienie danych uczestnika PPK do wybranej instytucji finansowej, z którą XYZ ma zawartą umowę o zarządzanie PPK oraz umowę o prowadzenie PPK, tj. Najlepsze PPK Na Świecie S.A. Poza tym dane będą ujawnione wyłącznie podmiotom współpracującym z XYZ, świadczącym usługi w zakresie wsparcia informatycznego lub personalnego.

Informujemy ponadto, że dane osobowe będą przechowywane przez okres niezbędny do archiwizacji dokumentacji, dotyczący przedawnienia roszczeń pracowniczych/związanych z uczestnictwem w PPK.

Osoba, której dane osobowe dotyczą, ma prawo dostępu do ich treści, wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, a dodatkowo prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także prawo do wniesienia sprzeciwu wobec przetwarzania oraz prawo do przenoszenia danych – wyłącznie w przypadkach przewidzianych w RODO.

Podanie danych osobowych uczestnika PPK jest wymogiem prawidłowej realizacji programu PPK. Bez ich podania XYZ nie będzie w stanie prawidłowo realizować obowiązków wynikających z ustawy o pracowniczych planach kapitałowych, a uczestnik PPK z kolei nie będzie mógł prawidłowo korzystać ze swoich uprawnień gwarantowanych przez PPK.

Ad. 2

Mając tak rozpisany obowiązek informacyjny, uzupełnienie rejestru czynności przetwarzania danych nie powinno być trudne. Zróbmy to na przykładzie czynności „gromadzenie i archiwizacja dokumentacji dotyczącej PPK".

Nazwę czynności już mamy, następny krok to wskazanie odpowiedzialnej za nią jednostki organizacyjnej. W wielu przypadkach będzie to dział kadr.

Potem mamy cel przetwarzania – w zasadzie będzie tożsamy z nazwą czynności, więc sprawa też prosta.

Kolejny punkt RCP to kategorie danych – wpisujemy pracowników i zleceniobiorców, następnie mamy kategorie danych – wskazujemy te, które znajdują się w dokumentacji PPK, którą musi archiwizować pracodawca.

Później określamy podstawę prawną – pamiętajmy, że mówimy tu o archiwizacji dokumentacji, a o tej niestety nic nie wspomina wskazana wcześniej ustawa z dnia 4 października 2018 r. o pracowniczych planach kapitałowych. Z pomocą przychodzi nam UODO - wg Prezesa UODO instytucja PPK jest ściśle powiązana z dokumentacją dotyczącą ustalania wymiaru wynagrodzenia, zatem okres przechowywania takiej dokumentacji wynosił będzie 10 lat, zgodnie z przepisami ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (art. 125a ust. 4a). Czyli mamy jednocześnie ustaloną zarówno podstawę prawną jak i okres retencji danych.

Jeśli chodzi o źródło danych to będzie to sam zainteresowany, a także pracodawca.

W omawianym przypadku nie mamy do czynienia z współadministrowaniem, wobec czego w tej części RCP wskazujemy, że „nie ma zastosowania".

Kolejny punkt to kwestia podmiotów przetwarzających – jeśli mamy outsourcing w tym zakresie np. obsługa kadrowo – płacowa, zewnętrzne archiwum, to wskazujemy właściwego procesora.

Dalej określamy systemy teleinformatyczne, środki bezpieczeństwa oraz wskazujemy czy konieczne jest przeprowadzenie DPIA, a także odnosimy się do kwestii transferu danych do państw trzecich.

Powyższe pola rejestru bazują na wzorze RCP udostępnionym przez Urząd Ochrony Danych Osobowych, warto zatem zapoznać się z tym materiałem. Natomiast przedstawiony przeze mnie opis będzie przydatny do wypełnienia poszczególnych pól informacyjnych dla interesującej nas czynności przetwarzania.

Ad. 3
Tak jak wskazałem wyżej – Prezes UODO wskazuje, że retencja danych dla PPK to 10 lat. Informacja ta znalazła się w newsletterze Urzędu nr 6/2019 z września 2019 r.

Ad. 4
Ocena ryzyka musi być przeprowadzona zawsze, natomiast DPIA tylko wówczas, gdy mówimy o wysokim ryzyku naruszenia praw lub wolności osoby, której dane dotyczą. W niniejszym artykule nie ma miejsca na dokładne przybliżenie tego tematu z uwagi na to, że stanowiłoby to tak naprawdę odrębny wpis blogowy. Wspomnę zatem, że do oceny ryzyka można wykorzystać np. normę ISO 27005 oraz ISO 31000.

Michał Sztąberek, Prezes iSecure Sp. z o.o.