Zasady przekazywania danych do państwa trzecich

W Specjalnym Ośrodku Szkolno-Wychowawczym Nr 1 nie przekazujemy danych osobowych pracowników, uczniów, rodziców oraz opiekunów prawnych do państw trzecich czy organizacji międzynarodowych.
W sytuacji gdyby taki wniosek został wystosowany należy zastosować poniższe instrukcje:
Aby zgodnie z RODO przekazać dane do państwa trzeciego – konieczne jest zastosowanie odpowiedniego mechanizmu transferu danych. Wybór mechanizmu transferu wymaga przeprowadzenia kilkuetapowej analizy oraz jej udokumentowania (aby zapewnić zgodność z zasadą rozliczalności). Stosowne regulacje znajdują się Rozdziale V RODO.

Należy jednak pamiętać, iż w pierwszej kolejności jednak – przekazywanie danych do państw trzecich powinno zostać ocenione przez pryzmat zgodności z ogólnymi zasadami ochrony danych osobowych, a dopiero potem – przez pryzmat zgodności z przepisami Rozdziału V.

Poniżej przedstawiamy najważniejsze etapy wyboru mechanizmu transferu danych do państw trzecich:

1. Czy odbiorca danych znajduje się w państwie trzecim?

Przed transferem danych do innego państwa, należy upewnić się, czy odbiorca danych znajduje się w państwie trzecim. Państwo trzecie w rozumieniu RODO to państwo spoza Europejskiego Obszaru Gospodarczego (EOG tworzą państwa Unii Europejskiej oraz Islandia, Liechtenstein i Norwegia). Warto zwrócić szczególną uwagę na współpracę z odbiorcami danych z Wielkiej Brytanii. W momencie wyjścia Wielkiej Brytanii z Unii Europejskiej, Wielka Brytania najprawdopodobniej stanie się państwem trzecim.

Prezes UODO wskazuje, iż na wypadek Brexitu, każdy administrator lub podmiot przetwarzający, którzy obecnie przekazują dane do Wielkiej Brytanii, powinni:

- zidentyfikować, jakie dane, w jakich celach i na jakiej podstawie prawnej są obecnie przekazywane do Wielkiej Brytanii;
- zdecydować, czy te transfery będą kontynuowane po Brexicie;
- wybrać i wdrożyć odpowiedni mechanizm, bądź podstawę prawną umożliwiającą przekazywanie danych;
- w razie potrzeby zmodyfikować wewnętrzną dokumentację przetwarzania danych, w tym rejestr czynności przetwarzania, klauzule informacyjne, istniejące wiążące reguły korporacyjne; a także -
- śledzić informacje dotyczące przebiegu procesu wyjścia Wielkiej Brytanii z UE, gdyż nie jest jeszcze pewne na jakich zasadach to nastąpi, co może mieć wpływ na obowiązki związane z transferem danych.[1]

2. Czy Komisja Europejska wydała decyzję stwierdzającą odpowiedni stopień ochrony?

Kolejnym krokiem jest wybór mechanizmu transferu danych do państwa trzeciego. W pierwszej kolejności należy sprawdzić, czy Komisja Europejska (KE) wydała decyzję potwierdzającą, że państwo trzecie zapewnia odpowiedni stopień ochrony. Dzięki takiej decyzji przekazywanie danych nie jest obwarowane dodatkowymi wymogami – w szczególności nie wymaga zezwolenia właściwego organu nadzoru ani wdrożenia szczególnych zabezpieczeń. Decyzje Komisji publikowane są w Dzienniku Urzędowym Unii Europejskiej. Aktualnie KE wydała takie decyzje w stosunku do następujących państw: Andora, Argentyna, Kanada, Wyspy Owcze, Guernsey, Izrael, Wyspa Man, Japonia, Jersey, Nowa Zelandia, Szwajcaria, Urugwaj oraz USA (w ramach Privacy Shield)[2].

3. Czy podmiot przekazujący dane zapewnia odpowiednie zabezpieczenia?

W przypadku braku decyzji KE, administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej. Celem jest zapewnienie analogicznej ochrony podmiotowi danych, jaka przysługiwałaby mu w sytuacji przetwarzania jego danych wewnątrz Unii Europejskiej.

Do odpowiednich zabezpieczeń należą:

- **Wiążące reguły korporacyjne** – czyli ustalone w ramach międzynarodowych grup przedsiębiorców zasady transferu danych, zatwierdzone przez organ nadzorczy, zgodnie z mechanizmem spójności; wiążące reguły korporacyjne są tworzone na potrzeby konkretnej grupy.
- **Standardowe klauzule ochrony danych** – są to standardowe klauzule umowne przyjęte przez Komisję Europejską lub przez organ nadzorczy i zatwierdzone przez KE. Klauzule te powinny zostać zawarte w umowie z odbiorcą danych; mogą one stanowić element innej umowy, np. o świadczenie usług. Klauzule publikowane są w formie decyzji KE w Dzienniku Urzędowym Unii Europejskiej.
- **Zatwierdzone kodeksy postępowania** – są to kodeksy postępowania mające pomóc we właściwym stosowaniu RODO, opracowane przez zrzeszenia i inne podmioty reprezentujące określone kategorie przedsiębiorców. Zastosowanie tego mechanizmu polega na zaakceptowaniu i przyjęciu takiego kodeksu przez podmiot z państwa trzeciego będący odbiorcą danych. Kodeks postępowania może być uznany za „odpowiednie zabezpieczenie" dopiero po zatwierdzeniu go przez właściwy organ nadzoru. Aktualnie w Polsce żaden ze zgłoszonych kodeksów nie został formalnie zatwierdzony przez Prezesa Urzędu Ochrony Danych Osobowych.
- **Zatwierdzony mechanizm certyfikacji** – czyli uzyskanie przez odbiorcę danych w państwie trzecim certyfikacji, mającej świadczyć o zgodności operacji przetwarzania z RODO.

Przekazanie danych w oparciu o wskazane powyżej zabezpieczenia nie będzie wymagać zgód organów nadzorczych.

- **Klauzule umowne między podmiotem przekazującym dane a odbiorcą danych w państwie trzecim** – mechanizm ten polega na zawarciu w umowie odpowiednich klauzul umownych zapewniających bezpieczeństwo danych osobowych oraz skuteczną realizację praw podmiotów danych. Niemniej jednak transfer danych z wykorzystaniem tego mechanizmu wymaga dodatkowego zezwolenia właściwego organu nadzoru.
- Podmiot planujący przekazanie danych osobowych do państw trzecich powinien przeanalizować, które z odpowiednich zabezpieczeń może znaleźć zastosowanie w określonej sytuacji. Wybór będzie zależał od tego, czy przekazanie danych odbywa się w ramach grupy przedsiębiorstw, czy odbiorca danych legitymuje się zatwierdzonym certyfikatem albo czy zechce podpisać umowę zawierającą odpowiednie klauzule ochrony danych bądź przyjąć właściwy kodeks postępowania. Oprócz wdrożenia odpowiednich zabezpieczeń należy dodatkowo zapewnić, iż transfer danych nie wpłynie negatywnie na możliwość skutecznego egzekwowania praw podmiotów danych.