

Transfery danych – co dalej?

Przekazywanie danych osobowych poza Europejski Obszar Gospodarczy (EOG) jest obecnie jednym z największych wyzwań w zakresie ochrony danych, z jakimi spotykają się przedsiębiorcy.

Rozwój technologii i związana z nim skala międzynarodowych transferów danych osobowych wpłynęły na obowiązujące standardy w zakresie ich zabezpieczenia. Niniejsza broszura stanowi krótkie podsumowanie aktualnych ram prawnych dotyczących przekazywania danych osobowych poza EOG, a także prezentuje podstawowe dostępne mechanizmy transferowe.

Regulacje dotyczące transferów danych osobowych

Przedsiębiorcy, którzy zamierzają przekazywać dane osobowe z Unii Europejskiej do państw spoza EOG powinni w pierwszej kolejności upewnić się, że poziom ochrony osób fizycznych zapewniony przez RODO nie zostanie naruszony przez planowany transfer oraz spełnić wymagania określone w rozdziale V RODO.

Co do zasady, transfer danych osobowych poza EOG jest zgodny z prawem, w sytuacji gdy:

- i. Komisja Europejska uznała, że dane państwo trzecie zapewnia **odpowiedni poziom ochrony** – poprzez tzw. „decyzję o adekwatności” (np. ostatnio wydana w odniesieniu do Wielkiej Brytanii) lub
- ii. przekazanie danych zabezpieczone jest poprzez odpowiednie **mechanizmy transferowe** (określone w art. 46 RODO) – np. standardowe klauzule umowne (SKU) przyjęte przez Komisję Europejską. Chociaż rozdział V RODO przewiduje również pewne alternatywne narzędzia przekazywania danych (inne niż SKU), np. wiążące reguły korporacyjne lub kodeksy postępowania, ich praktyczna użyteczność jest obecnie dość ograniczona.

W przypadku transferu danych osobowych poza EOG, przedsiębiorcy powinni więc sprawdzić, czy kraj odbiorcy danych został objęty decyzją o adekwatności. W przypadku braku takiej decyzji, należy zastosować odpowiednie zabezpieczenia, takie jak np. SKU. RODO przewiduje pewne odstępstwa od tego obowiązku (derogacje z art. 49 RODO), jednak mają one zastosowanie w wyjątkowych przypadkach.

Czym są nowe standardowe klauzule umowne?

4 czerwca 2021 roku Komisja Europejska opublikowała ostateczną decyzję wykonawczą przyjmującą nowe standardowe klauzule umowne (nowe SKU).

Poprzednia wersja SKU, przyjęta przed rozpoczęciem stosowania RODO, nie spełnia aktualnie obowiązujących wymogów w zakresie ochrony danych. Nie odpowiada ona również złożoności międzynarodowych przepływów danych, np. nie umożliwia dalszego przekazywania danych od podmiotu przetwarzającego do dalszego podmiotu przetwarzającego (*sub-processora*).

Nowe SKU nie tylko odpowiadają wymogom RODO, ale i obejmują wszystkie cztery rodzaje stosunków umownych, tj.:

- i. między administratorem a administratorem w państwie trzecim (C2C);
- ii. między administratorem a podmiotem przetwarzającym w państwie trzecim (C2P);
- iii. między podmiotem przetwarzającym a podmiotem przetwarzającym w państwie trzecim (P2P);
- iv. między podmiotem przetwarzającym a administratorem w państwie trzecim (P2C).

Pełna treść nowych klauzul dostępna jest [tutaj](#).

Od kiedy korzystać z nowych standardowych klauzul umownych?

Przedsiębiorcy powinni zacząć korzystać z nowych SKU dla nowych transferów po 27 września 2021 roku.

W przypadku istniejących transferów (tj. opartych o dotychczasowe SKU zawarte przed dniem 27 września 2021 r.), przedsiębiorcy mogą nadal korzystać z dotychczasowych SKU do 27 grudnia 2022 roku, ale wyłącznie pod tym warunkiem, że operacje przetwarzania stanowiące przedmiot umowy pozostaną niezmienione, a korzystanie z dotychczasowych SKU gwarantuje, że transfery te podlegają odpowiednim zabezpieczeniom.

Chociaż 18-miesięczny okres przejściowy na zastąpienie obecnie zawartych SKU ich nową wersją może wydawać się dość długi, to zalecamy jak najszybsze rozpoczęcie tego procesu.

Dobrym punktem wyjścia jest zidentyfikowanie wszystkich przypadków i relacji, które wiążą się z przekazaniem danych osobowych poza EOG, jak również wszystkich istniejących umów zawartych z odbiorcami danych z państw trzecich.

Czy zawarcie standardowych klauzul umownych jest wystarczające dla zapewnienia zgodności?

Jak podkreślił Trybunał Sprawiedliwości Unii Europejskiej (TSUE) w wyroku w sprawie Schrems II, przedsiębiorcy, którzy zamierzają opierać się na SKU (nawet ich nowej wersji) przy przekazywaniu danych osobowych poza EOG, powinni jednocześnie zapewnić osobie, której dane dotyczą poziom ochrony merytorycznie równoważny do tego gwarantowanego przez RODO. W praktyce oznacza to, że samo zawarcie SKU może nie być wystarczające dla zapewnienia legalności transferu.

Wnioski płynące z wyroku w sprawie Schrems II wzbudziły dużą niepewność rynku w zakresie zasad prawidłowego przekazywania danych osobowych poza EOG. Pewną wskazówką w tym zakresie okazały się być zalecenia Europejskiej Rady Ochrony Danych (EROD) w sprawie środków uzupełniających narzędzia przekazywania danych. EROD podkreśla konieczność poprzedzenia transferu analizą prawa państwa trzeciego. Wyróżnia także następujące rodzaje środków, których zastosowanie może uzupełniać przyjęty mechanizm transferowy:

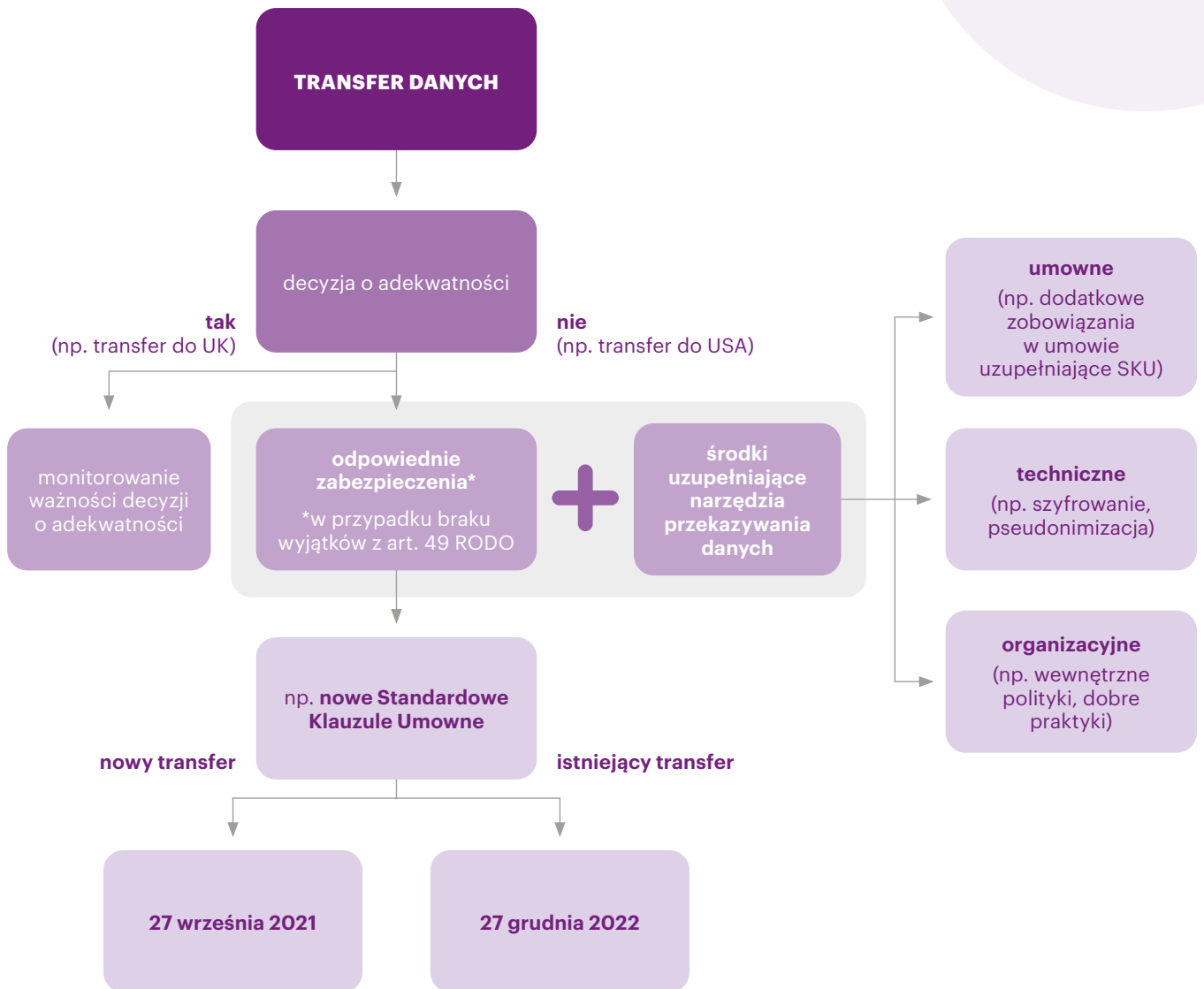
- i. umowne (np. dodatkowe klauzule w umowie z odbiorcą danych - uzupełniające SKU);
- ii. techniczne (np. szyfrowanie, pseudonimizacja);
- iii. organizacyjne (np. wewnętrzne polityki, dobre praktyki).

Wybór odpowiednich środków uzupełniających wymaga dogłębnego zrozumienia przepływu danych i indywidualnego podejścia do każdego przypadku.

Wybór odpowiednich środków uzupełniających wymaga dogłębnej analizy przepływu danych oraz indywidualnego podejścia do każdego przypadku.

Warto także dodać, że wdrożenie odpowiednich mechanizmów transferowych i środków uzupełniających może okazać się niezbędne nawet w sytuacji, gdy odbiorca nie ma fizycznego dostępu do danych osobowych (brak dostępu nie oznacza braku transferu danych). Wynika to z faktu, że nawet gdy dane są przekazywane np. w formie zaszyfrowanej, nadal mogą być one narażone na ryzyko, takie jak chociażby ich utraty.

Narzędzia transferowe w pigułce



Dlaczego zabezpieczanie transferów jest tak ważne?

Brak zabezpieczenia transferu danych może skutkować zwiększonym ryzykiem utraty, kradzieży lub ujawnienia danych osobom nieuprawnionym, co z kolei może nieść ze sobą niepożądane konsekwencje zarówno dla administratorów danych jak i osób, których dane osobowe zostały naruszone.

Potencjalne kary za naruszenie przepisów dotyczących transferu danych mogą okazać się dotkliwe (do 20 mln euro lub 4% rocznego przychodu, w zależności od tego, która z tych kwot jest wyższa), a szkody związane z ich nałożeniem nieodwracalne dla reputacji.

Jak zatem osiągnąć zgodność z przepisami dotyczącymi transferu danych?

Osiągnięcie zgodności z RODO wymaga analizy oraz dopasowania mechanizmów transferowych i środków je uzupełniających do konkretnego przepływu danych. Zespół Ochrony Danych Osobowych kancelarii Dentons ma duże doświadczenie w zakresie wdrażania rozwiązań transferowych dostosowanych do potrzeb Klienta. Nasza metodologia w tym zakresie podąża za zaleceniami EROD i obejmuje sześciostopniowy proces:

- i. **Mapowanie transferów danych** – Wspieramy Klientów w identyfikacji operacji przetwarzania danych osobowych, które wiążą się z ich transferem poza EOG;
- ii. **Weryfikacja narzędzia, na którym opiera się transfer Klienta** – Pomagamy w doborze odpowiedniego spośród mechanizmów transferowych określonych w art. 46 RODO, jak również identyfikujemy przypadki, w których transfer podlega derogacjom z art. 49 RODO;

- iii. **Ocena prawa lub praktyki państwa trzeciego** – Dzięki ścisłej współpracy z biurami Dentons na całym świecie, nasze wsparcie prawne uzupełniamy o analizę przeprowadzoną przez prawników kompetentnych do wydania opinii na gruncie prawa państwa trzeciego;
- iv. **Identyfikacja i przyjęcie środków uzupełniających** – Pomagamy Klientom w ocenie i wyborze umownych, technicznych i organizacyjnych środków uzupełniających do zastosowania w celu zapewnienia odpowiedniej ochrony danych osobowych;
- v. **Formalne kroki proceduralne** – Stale monitorujemy zalecenia EROD i w zależności od charakteru transferu doradzamy w zakresie dodatkowych kroków formalnych, które powinny zostać podjęte w związku z transferem;
- vi. **Ponowna ocena w odpowiednich odstępach czasu** – Pomagamy w dokonywaniu cyklicznej oceny przyjętych przez Klienta mechanizmów przekazywania danych osobowych poza EOG.

Sześciostopniowy proces opisany powyżej składa się na tzw. ocenę skutków transferu dla ochrony danych osobowych (**Transfer Impact Assessment – TIA**). Wdrożenie procesu TIA pozwala na udokumentowanie (a w przypadku ewentualnej kontroli wykazanie przed Urzędem Ochrony Danych Osobowych), że transfer poprzedzony został dokładną analizą, a zastosowane mechanizmy i środki uzupełniające w odpowiedni sposób mitygują potencjalne ryzyka z nim związane.

W razie jakichkolwiek pytań prosimy o kontakt – na Państwa życzenie z przyjemnością udzielimy dalszych informacji.

KEY CONTACTS



Karol Laskowski
Partner
+48 22 242 51 27
karol.laskowski@dentons.com



Dariusz Czuchaj
Counsel
+48 22 242 51 54
dariusz.czuchaj@dentons.com



Aleksandra Danielewicz
Senior Associate
+48 22 242 55 23
aleksandra.danielewicz@dentons.com



Anna Szczygiel
Associate
+48 22 242 58 64
anna.szczygiel@dentons.com



Paulina Węgrzynowicz
Associate
+48 22 242 52 52
paulina.wegrzynowicz@dentons.com