Warszawa, dnia 10 listopada 2021 r.

STANDARDOWE KLAUZULE UMOWNE – CZY WIEMY KIEDY, KTÓRE KLAUZULE NALEŻY STOSOWAĆ?

W czerwcu 2021 r. Komisja Europejska opublikowała dwa bardzo ważne dokumenty. Jeden z nich przedstawia wzorcową umowę powierzenia, a drugi stanowi podstawę legalizującą transfer do podmiotów mających swoją siedzibę poza Unią Europejską:
- w stosunku do których Komisja Europejska nie wydała decyzji stwierdzającej odpowiedni stopień ochrony na mocy art. 45 RODO (czyli kolokwialnie mówiąc - nie zostały zatwierdzone jako kraje „bezpieczne") oraz
- nie podlegają pod przepisy RODO.

Każdy ze wspomnianych dokumentów został wydany odrębną decyzją KE:

- Decyzja wykonawcza Komisji (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 (dalej Decyzja UE 2021/915);
- Decyzja wykonawcza Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (dalej Decyzja UE 2021/914).

W jaki sposób mogą one pomóc Inspektorowi Ochrony Danych? Czy administrator musi z nich korzystać? Czy polski Urząd Ochrony Danych Osobowych wydał standardowe klauzule umowne? Kiedy i w jaki sposób je stosować? Czy możemy korzystać jeszcze ze starych klauzul umownych do transferu danych poza EOG? O tym przeczytacie poniżej.

1. Wzorcowa umowa powierzenia

Czyli według nomenklatury RODOwskiej - standardowe klauzule umowne (SCC) służące powierzeniu danych osobowych wewnątrz Unii. Nie mylmy ich z SCC służącymi do transferu danych poza Unię. Opisywane w tym punkcie klauzule dotyczą relacji między powierzającym dane do przetwarzania a ich odbiorcą, czyli między administratorem a podmiotem przetwarzającym mającym siedzibę w UE. Takie klauzule mogą być wydane albo przez organy nadzorcze ds. ochrony danych, albo przez Komisję Europejską.

1.2. Wzorcowa umowa powierzenia wydana przez organ krajowy

Art. 28 ust. 8 RODO Organ nadzorczy może przyjąć standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z mechanizmem spójności, o którym mowa w art. 63.

Niektóre zagraniczne organy ochrony danych osobowych skorzystały z możliwości jaką daje im zacytowany powyżej art. 28 ust. 8 RODO. Przykładowo, w lipcu 2019 r. duńska Agencja Ochrony

iSecure Sp. z o.o. | www isecure.pl | fax +48 22 378 26 34 | Sąd Rejonowy dla m. st. Warszawy w Warszawie
ul. Sienna 72A lok. 214 | e-mail kontakt@isecure.pl | NIP 525-247-17-82 | XII Wydział Gospodarczy
00-833 Warszawa | tel +48 22 126 58 54 | REGON 14-22-29-729 | KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

Danych wydała swoje SCC dotyczące powierzenia danych, podobnie jak rok później niemiecki organ nadzorczy Badenii-Wirtembergii. Natomiast polski organ nie skorzystał z tego przepisu ani z dorobku krajów sąsiednich, co zrobił jego szwedzki odpowiednik. Mianowicie w kwietniu 2020 r. szwedzki organ nadzorczy wskazał, że duńskie standardowe klauzule umowne przetwarzania danych osobowych mogą być stosowane również w Szwecji.

1.3. Wzorcowa umowa powierzenia wydana przez Komisję Europejską

Komisja Europejska wydała własny wzór umowy powierzenia (Decyzja UE 2021/915). Nie oznacza to, że administratorzy powierzając dane procesorom muszą stosować ten dokument. Jest to dobrowolne (można, ale nie ma obowiązku korzystać z tego konkretnie wzoru), ale pamiętajmy, że nie służy do przekazywania danych do państw trzecich, czyli poza Unię.

Art. 28 ust. 7 RODO Komisja może określić standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.

Komisja Europejska w swoich klauzulach umownych zawarła wprost obowiązek zapewnienia prawidłowości i aktualności danych osobowych, który ma spoczywać na procesorze. To on powinien niezwłocznie poinformować administratora o nieprawidłowych lub nieaktualnych danych, co nieczęsto jest spotykane w powszechnie używanych umowach powierzenia. Ponadto załącznik nr 3 SCC wskazuje nam na sposób opisania stosowanych środków technicznych i organizacyjnych, wraz z przykładami. Środki powinny być opisane szczegółowo, a nie w sposób ogólny. Dokument zawsze może nam się przydać jako wzorcowy, gdy w negocjacjach nie możemy dojść do porozumienia z drugą stroną. Dlatego warto zaglądać do wzorcowych klauzul umownych, pod adres: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32021D0915.

Podsumowując pierwszą część artykułu pamiętajmy, że powyższe klauzule wydane na mocy Decyzji UE 2021/915 **dotyczą powierzenia danych między podmiotami mającymi siedzibę w UE - administratorem i podmiotem przetwarzającym**. Nie mamy obowiązku ich stosować.

2. Standardowe Klauzule Umowne dotyczące transferu danych

Chcąc transferować dane osobowe poza UE musimy rozejrzeć się za dodatkowymi rozwiązaniami wynikającymi z rozdziału V RODO, czyli w kolejności:

1) czy istnieje decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony w danym kraju trzecim?
2) czy podmiot potrafi zapewnić odpowiednie zabezpieczenia, w przypadku braku decyzji Komisji (np. przy pomocy wiążących reguł korporacyjnych lub SCC przyjętych przez Komisję Europejską)?
3) czy w przypadku braku powyższych podstaw zachodzi wyjątek określony w art. 49 RODO (np. wyraźna zgoda osoby, której dane są przesyłane poza Unię)?

W niniejszym artykule skupiamy się na nowych SCC legalizujących transfer poza UE, wydanych na mocy Decyzji UE 2021/914, ale przy okazji przypomnimy, że nadal można odnaleźć, które państwa zostały uznane przez Komisję za „bezpieczne" (wobec których Komisja Europejska wydała decyzję stwierdzającą odpowiedni stopień ochrony) – lista publikowana jest pod adresem:

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Natomiast SCC dotyczące transferu danych opublikowane w decyzji Komisji Europejskiej znajdują się pod tym linkiem: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32021D0914 i nie mogą być wydane przez organ krajowy do ochrony danych osobowych, więc nie szukajmy różnych wersji na stronach krajowych organów nadzorczych.

2.1 Proces podpisania nowych SCC. Kto z kim?

Po zweryfikowaniu, czy podmiot z którym chcemy rozpocząć współpracę nie posiada siedziby w kraju „bezpiecznym" (czyli co do którego Komisja Europejska wydała decyzję stwierdzający stopień ochrony), możemy zacząć zastanawiać się nad podpisaniem standardowych klauzul umownych. Najlepiej jest przeczytać motyw 7 Decyzji UE 2021/914, który uwzględnia, kiedy SCC mogą mieć zastosowanie.

Jednocześnie należy pamiętać, że jedną stroną umowy jest podmiot wysyłający dane, a drugą stroną podmiot je odbierający. Zarówno podmiot odbierający jak i wysyłający może pełnić różne role: być administratorem lub podmiotem przetwarzającym. Klauzule opublikowane przez Komisję składają się z modułów, które uwzględniają możliwe scenariusze wymiany danych. To znaczy, że w jednym dokumencie - Decyzji UE 2021/914, mamy umieszczonych kilka wariantów w celu zawarcia umowy między:

1) administratorem a administratorem (moduł pierwszy);
2) administratorem a podmiotem przetwarzającym (moduł drugi);
3) podmiotem przetwarzającym a dalszym podmiotem przetwarzającym (moduł trzeci);
4) podmiotem przetwarzającym a administratorem (moduł czwarty).

Musimy przy tym pamiętać, że w przypadku stosowania tych SCC mówimy o sytuacji, kiedy podmiot odbierający dane nie podlega pod przepisy RODO, co wynika z motywu 7 decyzji 2021/914.

2.2. Jak stworzyć umowę?

Gdy spojrzymy do Decyzji UE 2021/914 zauważymy kilka motywów, artykułów wstępnych i właściwe moduły (znajdujące się w 4 sekcjach) – w zależności kto z kim podpisuje umowę, np. czy administrator z administratorem czy administrator z podmiotem przetwarzającym.

Tworząc umowę należy pamiętać o kilku następujących zasadach:

1) zweryfikujmy jakie role pełnią podmioty, aby móc dopasować odpowiedni moduł,
2) upewnijmy się, że strona odbierająca dane z mocy prawa nie będzie podlegała pod RODO,
3) pamiętajmy, że klauzule nie są modyfikowalne (zgodnie z klauzulą 2).

Chociaż klauzule nie są modyfikowalne, to można uzupełnić je o dodatkowe informacje, załączniki, czy włączyć SCC do szerszej umowy podpisywanej z drugim podmiotem (lub w ramach umowy adhezyjnej w związku z przyjęciem regulaminu wraz z SCC przedstawionego przez drugą stronę).

Klauzule 1-7 nie posiadają budowy modułowej (z wyjątkiem klauzuli 3 lit. A) pkt (ii), (iii), (iv), (viii) – na co prosimy uważać), natomiast kolejne klauzule należy dobierać według poszczególnych modułów, właściwych dla ról przyjętych przez podmioty je podpisujące.

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

Klauzula 7 jest fakultatywna, jednak dodając ją do naszej umowy uchroni nas od konieczności aneksowania umowy w przyszłości, gdybyśmy chcieli dodać kolejną stronę do umowy. Mianowicie dzięki tej klauzuli wystarczy dodać kolejną stronę umowy w załączniku I (część A), a strona podpisując załącznik I staje się zobligowana do przestrzegania zasad wynikających z SCC.

Pozostałe załączniki zawierają miejsce na opisanie przekazywanych danych, wskazanie właściwego organy, zastosowanie środków technicznych i organizacyjnych oraz wykaz podwykonawców.

2.2 Czy musimy podpisać nowe SCC gdy korzystamy ze starych?

Przeprowadzając audyt w firmach możemy trafić na stare SCC, sprzed ponad 10 lat, podpisane między spółkami w grupie. Czy powinny one pomyśleć nad podpisaniem nowych klauzul opublikowanych w czerwcu 2021 r.? To zależy od kilku czynników. Jeżeli umowa nie uległa zmianie i przetwarzane są cały czas te same dane, a ich przekazanie odbywa się z zastrzeżeniem odpowiednich zabezpieczeń to do 27 grudnia 2022 r. możemy korzystać z wcześniejszych klauzul. Nie musimy ich aneksować, jednakże należy wcześniej zacząć procesować podpisanie nowych SCC, ponieważ należy porozumieć się do ich treści z drugą stroną oraz sprawdzić czy zapewnienia drugiej strony będą mogły być realizowane (TIA). Aktualnie możemy zauważyć na stronach dużych dostawców chmurowych (czy społecznościowych), że zawierają już w swoich regulaminach/warunkach świadczenia usług nowe SCC. Ponadto, przykładowo Microsoft (w ramach MS Teams), umożliwia podjęcie decyzji co do lokalizacji danych.

2.3. W jaki sposób przeprowadzić ocenę ryzyka transferu danych?

Transfer Impact Assessment wynika z klauzuli 14 nowych SCC. Według regulacji strony umowy gwarantują, że nie ma podstaw, by uważać, iż prawa i praktyki w państwie odbiorcy danych (mającym siedzibę poza Unią Europejską), uniemożliwiały podmiotowi odbierającemu dane wypełnienie jego obowiązków wynikających z klauzul. Proszę zauważyć, że to strony składają oświadczenie, że należycie uwzględniły m. in. cel przetwarzania danych, długość łańcucha przetwarzania czy miejsce przechowywania i przekazywania danych, a podmiot odbierający dane przyjmując SCC gwarantuje, że przeprowadzając ocenę na podstawie uwzględnionych zmiennych, dołożył wszelkich starań, aby udostępnić podmiotowi przekazującemu dane odpowiednie informacje. Co oznacza, że dokonując ocenę ryzyka transferu danych powinniśmy współpracować z podmiotem odbierającym dane, znajdującym się w kraju poza UE. W końcu najlepiej znają swoje prawodawstwo oraz sposób przetwarzania danych w swoich systemach przy pomocy zabezpieczeń organizacyjnych i technicznych. Taka ocena ryzyka powinna być udokumentowana, o czym stanowi klauzula 14 lit. d) w brzmieniu:

> Klauzula 14 lit. d) SCC
> Strony zgadzają się udokumentować ocenę, o której mowa w lit. b), i udostępnić ją na żądanie właściwego organu nadzorczego.

Ocena ryzyka powinna uwzględniać elementy wymienione w klauzuli 14, z uwzględnieniem art. 23 RODO. Jak już zostało wspomniane, należy zweryfikować np. cel przetwarzania danych, długość łańcucha przetwarzania, miejsce przechowywania danych czy zastosowane środki organizacyjne i techniczne w celu zapewnienia realizacji klauzul.

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

2.4. Zakończenie.

Podsumowując transfer danych poza EOG pamiętajmy, że proces zawarcia umowy na bazie standardowych klauzul umownych może trwać – chociażby ze względu na konieczność wykonania razem z drugą stroną oceny ryzyka uwzględniającej transfer danych (w tym poznania podwykonawców strony odbierającej dane) czy zaakceptowania środków bezpieczeństwa, które należy wymienić w załączniku II SCC.

Już dzisiaj możemy podpisać nowe standardowe klauzule umowne, dlatego nie czekajmy do 27 grudnia 2022 r. Oczywiście w przypadku pytań czy pomocy zapraszamy do kontaktu.

Przemysław Siarka, Specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł