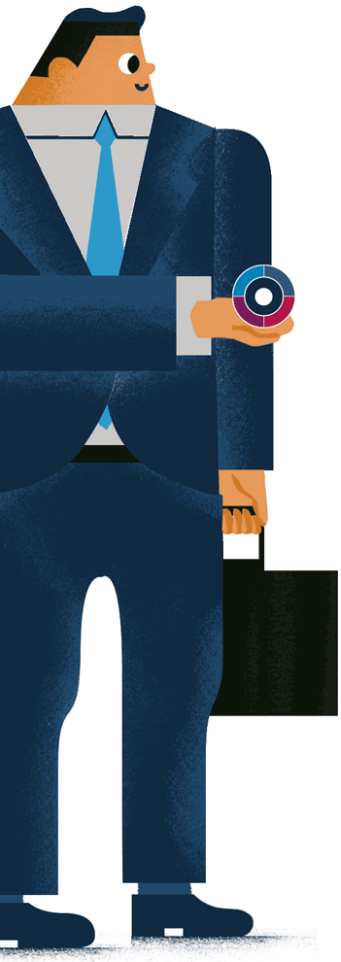
NIEOFICJALNE TŁUMACZENIE - 24 VII 2022 r.

STANDARDOWE KLAUZULE UMOWNE (SCC)

Pytania i odpowiedzi Komisji Europejskiej



4 czerwca 2021 r. Komisja Europejska przyjęła dwa zestawy standardowych klauzul umownych (SCC), pierwszy służący do stosowania między administratorami danych,
a podmiotami przetwarzającymi dane w ramach Europejskiego Obszaru Gospodarczego (EOG), oraz drugi służący do przekazywania danych osobowych do krajów spoza EOG.

Aby pomóc we właściwym zrozumieniu i stosowaniu SCC Komisja opublikowała także odpowiedzi na najczęstsze pytania dotyczące tego narzędzia.

WERSJA ONLINE

Spis treści

Pytania i odpowiedzi

I. STANDARDOWE KLAUZULE UMOWNE - INFORMACJE OGÓLNE

1. Co to są Standardowe Klauzule Umowne?

Standardowe Klauzule Umowne (SCC) to **znormalizowane** i **zatwierdzone wzorcowe klauzule ochrony danych,** które umożliwiają administratorom i podmiotom przetwarzającym, wypełnianie obowiązków wynikających z unijnych przepisów o ochronie danych. SCC mogą być włączane przez administratorów i podmioty przetwarzające do umów zawieranych z kontrahentami. **Nie ma obowiązku stosowania SCC**. Klauzule te **są stosowane dobrowolnie,** w celu wykazania zgodności z wymogami w zakresie ochrony danych; zastosowanie klauzul wymaga umownego zobowiązania do ich przestrzegania. Komisja Europejska jest uprawniona do przyjmowania treści SCC (1) w relacji między administratorami danych a podmiotami przetwarzającymi dane oraz (2) wykorzystywanych do transferu danych osobowych poza EOG.

2. Jakie Standardowe Klauzule Umowne zostały przyjęte przez Komisję Europejską?

4 czerwca 2021 r. Komisja przyjęła **dwa zestawy Standardowych Klauzul Umownych** (**SCC**).

(1) **SCC dotyczące relacji między administratorami, a podmiotami przetwarzającymi,** które spełniają wymogi określone w art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych, "RODO") oraz w art. 29 ust. 3 i 4 rozporządzenia (UE) 2018/1725 (rozporządzenie o ochronie danych mające zastosowanie do instytucji, organów, urzędów i agencji UE, "EUDPR"). W związku z tym, SCC mogą być stosowane przez podmioty publiczne i prywatne, a także przez instytucje, organy, urzędy i agencje UE. W ten sposób SCC zapewniają spójne podejście do relacji między administratorami, a podmiotami przetwarzającymi - w całym EOG. Standardy SCC są dostępne tutaj: https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors

(2) **SCC stanowi także narzędzie do transferu danych**, tj. do spełniania wymogów RODO, w zakresie **przekazywania danych osobowych do krajów spoza EOG**. Niniejsze SCC, zawierają zabezpieczenia w zakresie ochrony danych, mające na celu zapewnienie, że dane osobowe korzystać będą z wysokiego poziomu ochrony, pomimo transferu poza EOG. SCC mogą być one stosowane przez podmioty przekazujące dane, **bez konieczności uzyskania uprzedniego**

zezwolenia organu nadzorczego (na transfer danych lub zastosowanie konkretnych klauzul). Przystępując do SCC, podmioty odbierające dane danych zobowiązują się umownie, do przestrzegania szeregu środków ochrony danych. Treść SCC jest dostępna pod następującym linkiem: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_pl

3. Jakie są zalety stosowania SCC?

Dzięki standaryzacji i wstępnemu zatwierdzeniu, SCC **są gotowym narzędziem,** które jest łatwe do wdrożenia. Jest to szczególnie ważne dla MŚP lub mikroprzedsiębiorców, którzy mogą nie dysponować zasobami, umożliwiającymi negocjowanie indywidualnych umów z każdym ze swoich partnerów handlowych. To co odróżnia SCC od innych mechanizmów zgodności, to brak konieczności uprzedniego zatwierdzenia przed zastosowaniem, przez krajowy organ nadzorczy, a także niższe koszty, w porównaniu konkurencyjnych mechanizmów, których wdrożenie jest zazwyczaj bardziej kosztowne (np. systemy certyfikacji).

Informacje zwrotne pozyskiwane od zainteresowanych stron wskazują, że **SCC w zakresie transferu danych** są zdecydowanie **najczęściej wykorzystywanym instrumentem transferu danych** przez europejskie przedsiębiorstwa**.** Na przykład, zgodnie z rocznym raportem IAPP-EY dotyczącym zarządzania prywatnością w 2019 r., "najpopularniejsze tych narzędzi transferowych to w przeważającej większości standardowe klauzule umowne, 88% respondentów tegorocznego badania wskazało SCC, jako główną metodę transgranicznego przekazywania danych [...]".

4. Jaki proces został zastosowany przez Komisję Europejską przy opracowywaniu SCC?

Przygotowując dwa zestawy SCC, Komisja starała się uzyskać **stanowiska zainteresowanych stron,** aby lepiej zrozumieć realia oraz rzeczywiste potrzeby, oraz wyciągnąć wnioski z praktycznych doświadczeń w dotychczasowym stosowaniu istniejących SCC. Komisja otrzymała szczegółowe informacje zwrotne od zainteresowanych stron (w tym od przedstawicieli branży, społeczeństwa obywatelskiego, prawników i pracowników akademickich), za pośrednictwem Wielostronnej Grupy Ekspertów ds. RODO[1], szeroko zakrojonych konsultacji społecznych[2], specjalnych warsztatów, paneli dyskusyjnych oraz niezależnych badań, zleconych instytucjom zewnętrznym.

5. Czy Komisja Europejska oceni po jakimś czasie, jak nowe SCC działają w praktyce?

[1] Więcej informacji można znaleźć na stronie: https://ec.europa.eu/transparency/expert-groups-register/screen/expertgroups/consult?do=groupDetail.groupDetail&groupID=3537.

[2] Zobacz: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Data-protectionstandard-contractual-clauses-for-transferring-personal-data-to-non-EU-countries-implementing-act-_en oraz https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12740-Data-protection-standardcontractual-clauses-between-controllers-&-processors-located-in-the-EU-implementing-act-_en.

Artykuł 97 RODO nakłada na Komisję **obowiązek przeprowadzania przeglądu procesu wdrażania RODO, co cztery lata** (sprawozdanie z oceny za rok 2020 jest dostępne tutaj https://ec.europa.eu/info/law/law- topic/data-protection/communication-two-years-applicationhttps://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_engeneral-data-protection-Regulation_en). **Kolejny przegląd będzie miał miejsce do 2024 r.** i będzie obejmował także ocenę praktycznego zastosowania SCC.

ZAWARCIE, MODYFIKACJE I ZWIĄZEK Z INNYMI POSTANOWIENIAMI ZAWIERANYCH UMÓW

6. Czy istnieją szczególne wymagania dotyczące zawierania przez strony SCC?

Wykorzystanie SCC w celu spełnienia wymogów RODO i EUDPR w relacji administrator – podmiot przetwarzający, lub jako narzędzia transferu danych, wymaga zawarcia przez strony umowy. W tym celu strony muszą wypełnić załączniki do SCC, które stanowią integralną część klauzul. **Strony muszą** między innymi **wskazać** swoje dane kontaktowe oraz informacje o pełnionych rolach (kto pełni funkcję administratora i podmiotu przetwarzającego lub podmiotu przekazującego i podmiotu odbierającego dane) w ramach klauzul. SCC nie zawierają żadnych wymogów co do sposobu sformalizowania zawarcia umowy (np. czy można zawrzeć umowę elektronicznie). Pozostawia się to w gestii **prawa krajowego, któremu podlega umowa**.

7. Czy treść SCC może zostać zmieniona?

Treść SCC nie może być zmieniana, **z wyjątkiem** (i) **wyboru modułów i/lub konkretnych alternatywnych opcji przedstawionych w treści**, (ii) **uzupełnienia tekstu w** razie potrzeby (zasygnalizowanej nawiasami kwadratowymi), np. wskazania właściwego sądu lub organu nadzorczego oraz określenia terminów, (iii) **wypełnienia załączników** lub (iv) wprowadzenia **dodatkowych zabezpieczeń** zwiększających poziom ochrony danych. Powyższych zmian nie uważa się niedozwoloną zmianę treści zasadniczej SCC.

Uwaga dla administratorów i podmiotów przetwarzających: jeśli strony zmienią treść SCC (poza zmianami, o których mowa poniżej), nie mogą one polegać na pewności prawnej oferowanej przez akt prawny UE.

W treści SCC strony muszą dokonać niezbędnych zmian, wybierając jedną z dwóch opcji, dotyczących:

- zgodności z RODO lub zgodności z EUDPR;
- zastosowania uprzedniego i szczególnego upoważnienia subprocesora(-ów) lub ogólnego pisemnego upoważnienia do dalszego powierzenia danych subprocesorowi(-om).

Uwaga w przypadku transferu danych: jeśli strony zmienią treść SCC (tj. poza wyborem odpowiednich modułów i/lub opcji oraz wypełnieniem informacji w nawiasach kwadratowych i wypełnieniem załączników), zmodyfikowane klauzule nie mogą już być wykorzystywane, jako podstawa do transferu danych do państw trzecich, chyba że zostaną zatwierdzone przez krajowy organ nadzorczy jako "klauzule *ad hoc*" (zgodnie z art. 46 ust. 3 lit. a) RODO).

8. Czy możliwe jest dodanie dodatkowych klauzul do SCC lub włączenie SCC do umowy głównej?

Strony mogą **uzupełnić SCC** dodatkowymi klauzulami lub **włączyć** je do szerszej umowy głównej, **o ile** inne postanowienia umowy głównej **nie są sprzeczne z SCC,** bezpośrednio lub pośrednio, ani nie naruszają praw osób, których dane dotyczą.

Przykład: *jeżeli postanowienia SCC wymagają od stron wzajemnego informowania się lub współpracy, strony mogą uzgodnić dodatkowe postanowienia określające, w jaki sposób w praktyce będzie przebiegać komunikacja/współpraca między stronami .*

Przykład: *zgodnie z postanowieniami SCC, podmiot odbierający dane ma obowiązek powiadomić podmiot przekazujący dane o naruszeniu ochrony danych, bez zbędnej zwłoki po powzięciu wiadomości o naruszeniu. Strony mogą określić ramy czasowe, w jakich takie powiadomienie musi zostać dostarczone, bez naruszania ogólnej zasady (tj. bez zbędnej zwłoki, ale nie później niż 72 godziny odkąd odbierający dane dowiedział się o naruszeniu).*

Przykład: *Klauzula 7.7 (w SCC dla administratorów i podmiotów przetwarzających), nakłada na podmiot przetwarzający obowiązek uzyskania upoważnienia od administratora, w celu zaangażowania podwykonawcy przetwarzania. Strony nie mogą zawrzeć w umowie głównej postanowień, które pozwalałyby podmiotowi przetwarzającemu dalej powierzyć dane, bez obowiązku konsultacji z administratorem, bądź zażądać od administratora udzielenia upoważnienia dalszego procesora, ponieważ takie postanowienie będzie bezpośrednio sprzeczne z klauzulą 7.7 SCC.*

9. Czy strony mogą usunąć moduły i/lub opcje, które nie mają zastosowania w konkretnym przypadku?

Strony powinny zachować w treści tylko te klauzule, które są istotne dla konkretnych okoliczności. Moduły i/lub opcje, które nie mają zastosowania, należy usunąć.

Przykład: *administrator chce przekazać dane osobowe innemu administratorowi, opierając się na SCC dla transgranicznych transferów danych. Wszystkie klauzule o charakterze ogólnym (dla których nie wskazano modułów np. sekcja I), a także klauzule istotne dla modułu 1, powinny zostać wyodrębnione i pozostawione. Wszystkie pozostałe klauzule, które odnoszą się do innych modułów, mogą zostać usunięte.*

Przykład: *w klauzuli 7.7 SCC zawieranych między administratorami a podmiotami przetwarzającymi (wykorzystanie subprocesorów), strony muszą wybrać jedną z dwóch opcji*

upoważnienia do korzystania z subprocesorów przez podmiot odbierający dane. Jeżeli strony wybiorą opcję 1, opcja 2 powinna zostać usunięta z treści SCC.

Przykład: *firma z siedzibą w EOG, będąca administratorem danych, chce nawiązać stosunek umowny z podmiotem przetwarzającym dane w EOG. W celu zachowania zgodności z art. 28 ust. 3 i 4 RODO, można zastosować wzór SCC, zawierany pomiędzy administratorami danych a podmiotami przetwarzającymi. W takim przypadku należy wybrać WARIANT 1 (który odnosi się do RODO) - i usunąć odniesienia do WARIANTU 2 (który dotyczy zgodności z EUDPR).*

10. W jaki sposób włączyć treść SCC do umowy głównej?

W celu zgodnego z prawem zastosowania SCC i zapewnienia przejrzystości, zawierane SCC muszą być wiążące dla wszystkich stron zawieranej umowy, zgodnie z wymogami prawa cywilnego danej jurysdykcji. Ponadto, SCC należy dostosować zaistniałych okoliczności (np. do transferów danych), poprzez wypełnienie załączników i wskazanie (stronom, a także zainteresowanym osobom, właściwym organom nadzorczym i sądom), które moduły, opcje i dodatkowe informacje (ujęte w nawiasach kwadratowych) zostały wybrane.

ZMIANY DOTYCZĄCE STRON

11. Jaki jest cel "klauzuli dokującej"?

„Klauzula dokująca" jest klauzulą **opcjonalną,** za pomocą której strony SCC mogą uzgodnić, iż w przyszłości do umowy **mogą przystąpić dodatkowe strony.** Zapewnia to stronom dodatkową elastyczność, w przypadku zmian w przyszłości podmiotów, które uczestniczą w porozumieniu dotyczącym przetwarzania (np. w przypadku, gdy konieczne staje się rozszerzenie łańcucha przetwarzania, poprzez włączenie kolejnego subprocesora).

Przykład: podmiot przetwarzający oferuje te same usługi kilku administratorom. Kilka lat po zawarciu SCC z jednym administratorem, w celu zapewnienia zgodności z art. 28 RODO, strony zgadzają się, że kolejny administrator może przystąpić do umowy, korzystając z klauzuli dokującej.

Przykład: *administrator przekazuje dane osobowe podmiotowi przetwarzającemu działającemu w państwie trzecim, na podstawie SCC dla transgranicznych transferów danych (z wykorzystaniem Modułu 2). W sytuacji, w której podmiot przetwarzający zechce zatrudnić subprocesora, strony uzgadniają, że subprocesor powinien przestrzegać pierwotnie zawartych SCC (korzystając z Modułu 3).*

12. Jak w praktyce działa klauzula dokująca? Czy istnieją jakieś wymogi formalne dotyczące przystąpienia nowych stron do umowy?

Jedna lub kilka nowych stron może przystąpić do SCC za zgodą wszystkich dotychczasowych stron SCC. SCC nie określa wymogów formalnych takiej zgody, przy czym zgoda powinna być wyrażona z uwzględnieniem obowiązujących przepisów prawa krajowego. Na przykład, o ile zezwala na to obowiązujące prawo, jedna strona może zostać upoważniona przez pozostałe strony, do wyrażania zgody na przystąpienie nowego podmiotu do SCC. Po uzyskaniu takiej zgody, nowa strona będzie musiała uzupełnić załączniki i **podpisać SCC wraz załącznikiem**. Zmiana tylko umowy głównej, której załącznikiem jest SCC, polegająca na dodaniu nowych stron do umowy głównej, nie jest wystarczająca do przystąpienia nowych stron do SCC.

13. Co się dzieje, gdy nowa strona przystępuje do SCC? Czy istnieje obowiązek dopełnienia dodatkowych formalności?

Po przystąpieniu do SCC nowa strona wstępuje we **wszystkie prawa i obowiązki, stosownie do swojej roli** (np. podmiot przekazujący lub odbierający dane, administrator danych lub podmiot przetwarzający). **Pozostałe strony mają jednocześnie odpowiednie prawa i obowiązki, w stosunku do nowej strony** (np. obowiązek udzielania pomocy przy odpowiadaniu na wnioski osób, których dane dotyczą itp.)

Załączniki do SCC muszą być **aktualizowane** po dodaniu nowych stron. Na przykład po przystąpieniu nowych stron należy wymienić te strony oraz ich role, a w stosownych przypadkach, także odpowiednio zaktualizować opis transferów i zastosowanych środków technicznych i organizacyjnych.

II. STANDARDOWE KLAUZULE UMOWNE, ZAWIERANE MIĘDZY ADMINISTRATORAMI DANYCH, A PODMIOTAMI PRZETWARZAJĄCYMI

14. Jaka jest różnica między SCC przyjętymi przez organy nadzorcze poszczególnych krajów, a SCC przyjętymi przez Komisję?

Artykuł 28 ust. 8 RODO upoważnia **krajowe organy nadzorcze,** do przyjęcia wzorów SCC stosowanych relacji pomiędzy administratorami, a podmiotami przetwarzającymi. Jeżeli krajowy organ nadzorczy przyjmie swoje SCC, mają one zastosowanie wyłącznie na terytorium właściwości tego organu. To, czy inne organy nadzorcze zaakceptują zastosowanie takich SCC, zależy od indywidualnych decyzji tych organów.

Dla odmiany, SCC przyjęte przez **Komisję zgodnie z** art. 28 ust. 7 RODO, można stosować w całym EOG - jako wiążące dla wszystkich organów nadzorczych w EOG. Ważność SCC przyjętych przez Komisję, może zostać zakwestionowana jedynie przed Trybunałem Sprawiedliwości Unii Europejskiej. SCC przyjęte przez Komisję zapewniają zharmonizowane podejście w całym EOG oraz pewność prawną aktu UE.

15. W jakiej formie instrukcje administratora powinny być przekazywane podmiotowi przetwarzającemu?

Zgodnie z klauzulą 7.1 "Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora ". SCC **nie precyzuje**, w jakiej formie należy przekazywać instrukcje, dlatego administrator danych może zdecydować się na przekazywanie instrukcji w dowolnej formie, jaką uzna za stosowną (np. pisemnie lub ustnie, za pomocą Internetu bądź innych form komunikacji), ale **pod warunkiem, że instrukcje te zostaną udokumentowane**.

16. Czy podmiot przetwarzający ma obowiązek poinformowania administratora, o subprocesorze(-ach), którego(-ych) angażuje?

Tak. Zgodnie z klauzulą 7.7 **strony muszą wybrać jedną z dwóch opcji**: WARIANT 1: wcześniejsze szczegółowe upoważnienie lub WARIANT 2: OGÓLNE PISEMNE UPOWAŻNIENIE. **W obu przypadkach** podmiot **przetwarzający musi przekazać** administratorowi **nazwę(-y) poszczególnych subprocesorów,** aby administrator mógł podjąć decyzję o autoryzacji wybranych subprocesorów. Nie wystarczy, aby przetwarzający podał tylko kategorie subprocesorów. **Do stron** należy **uzgodnienie terminu, w jakim podmiot przetwarzający** ma złożyć wniosek o uprzednie szczególne upoważnienie (WARIANT 1), **lub terminu poinformowania** administratora o wszelkich zamierzonych zmianach w uzgodnionym wykazie subprocesorów (WARIANT 2).

17. Co się stanie, jeżeli administrator zgłosi sprzeciw wobec zmian subprocesorów, w przypadku ogólnego upoważnienia na zaangażowanie subprocesorów?

Zgodnie z WARIANTEM 2 w klauzuli 7.7 SCC, podmiot przetwarzający musi wyraźnie poinformować administratora danych na piśmie, o wszelkich planowanych zmianach w uzgodnionym wykazie podwykonawców przetwarzania danych, przestrzegając uzgodnionego okresu powiadomienia. Jeżeli administrator sprzeciwia się planowanym zmianom, podmiot przetwarzający nie może zaangażować nowego subprocesora (lub nowych subprocesorów).

18. W jakim terminie podmiot przetwarzający musi powiadomić administratora o naruszeniu ochrony danych?

SCC nie określają terminu, w którym podmiot przetwarzający musi powiadomić administratora o naruszeniu ochrony danych, w przypadku gdy naruszenie dotyczy danych przetwarzanych przez podmiot przetwarzający. Klauzula 9.2 SCC precyzuje, że powiadomienie powinno nastąpić "bez zbędnej zwłoki". Określenie tego terminu należy zatem do stron, z uwzględnieniem szczególnych okoliczności przetwarzania.

19. W inny jaki sposób, oprócz audytu, podmiot przetwarzający może wykazać zgodność z wymaganiami wynikającymi z SCC?

Podmiot przetwarzający może skorzystać z innych mechanizmów, aby wykazać administratorowi, że prawidłowo wypełnia swoje obowiązki określone w SCC, bądź wynikające bezpośrednio z RODO, np. poprzez przestrzeganie **zatwierdzonego kodeksu postępowania zgodnie z** art. 40 RODO lub **zatwierdzonego mechanizmu certyfikacji zgodnie z** art. 42 RODO. Należy przy tym zauważyć, iż nie ma to wpływu na możliwość podjęcia przez administratora decyzji, o audycie czynności przetwarzania, które są objęte SCC.

III. STANDARDOWE KLAUZULE UMOWNE DOTYCZĄCE PRZEKAZYWANIA DANYCH DO PAŃSTW TRZECICH

PRZYCZYNY NOWELIZACJI I GŁÓWNE ZMIANY

20. Dlaczego Komisja znowelizowała poprzednie SCC w zakresie transferu danych do państw trzecich?

Na mocy poprzedniej **dyrektywy o ochronie danych** (dyrektywa 95/46/WE) Komisja przyjęła **trzy zestawy SCC:** dwa służące do przekazywania danych przez administratora działającego w EOG do administratora działającego poza EOG (decyzje Komisji 2001/497/WE i 2004/915/WE) oraz jeden służący do przekazywania danych przez administratora działającego w EOG do podmiotu przetwarzającego działającego poza EOG (decyzja Komisji 2010/87/UE).

Poprzednie SCC pozostały dostępne po wejściu w życie RODO, niemniej zaistniała **potrzeba dostosowania ich do nowych ram prawnych,** w szczególności aktualizacji w świetle nowych wymogów RODO oraz uwzględnienia zmieniającego się orzecznictwa Trybunału Sprawiedliwości UE (np. tzw. wyrok *Schrems II* w sprawie C-311/18).

Ponadto, **poprzednie SCC nie były już dostosowane do realiów nowoczesnej gospodarki cyfrowej**, charakteryzującej się zróżnicowanymi realiami czasu przetwarzania oraz długimi i często złożonymi łańcuchami przetwarzania, z udziałem wielu podmiotów, niekiedy ze zmieniającymi się rolami. Zaistniała zatem potrzeba **zmodernizowania "architektury"** dotychczasowych SCC, aby uczynić je bardziej przyjaznymi dla korzystających z nich, objąć nimi dodatkowe scenariusze transferów (takie jak transfery przez procesora do dalszego procesora), oraz zapewnić dodatkową elastyczność, poprzez umożliwienie przystępowania nowych stron w trakcie obowiązywania umowy.

21. Co nowego w porównaniu z poprzednimi SCC?

W nowych klauzulach **zachowano podstawowe elementy**, które zawarte były w SCC przyjętych na mocy poprzedniej dyrektywy o ochronie danych. Na przykład, zobowiązania

dotyczące podstawowych zasad ochrony danych, zobowiązania w zakresie bezpieczeństwa, zagadnienia dotyczące praw osób trzecich oraz jurysdykcji sądów i organów. Równocześnie wprowadzono **istotne zmiany.**

Po pierwsze, uaktualniono **„architekturę”** SCC, p..:

- SCC obejmują **dodatkowe scenariusze przekazywania** danych: podczas gdy zakres zastosowania poprzednich SCC był ograniczony do transferu danych: od administratora do administratora, oraz od administratora do procesora. Zmodernizowane SCC mogą być stosowane we wielu przypadkach transferu: od administratora do administratora (Moduł 1), od administratora do procesora (Moduł 2), od procesora do procesora (Moduł 3) oraz od procesora do administratora (Moduł 4).
- Trzy odrębne zestawy SCC, obejmujące dwa scenariusze transferu danych, zostały zastąpione **jednym zestawem SCC o strukturze modułowej** (obejmującym cztery scenariusze transferu). Strony muszą połączyć postanowienia o charakterze ogólnym (które mają zastosowanie niezależnie od konkretnego scenariusza) z modułem lub modułami, które mają zastosowanie w konkretnej sytuacji.
- **Klauzula dokująca** umożliwia dołączanie nowych stron do zawartych SCC, przez cały okres obowiązywania umowy.
- Uzupełnieniem SCC są **załączniki,** które są uzupełniane o konkretne informacje na temat konkretnych transferów, np. lista stron i ich ról, opis celu każdego indywidualnego transferu danych w ramach umowy, wykaz zastosowanych środków bezpieczeństwa, zabezpieczenia stosowane do ochrony danych wrażliwych itp.

Po drugie, wprowadzono **szereg zmian merytorycznych,** np.:

- SCC odzwierciedlają **nowe wymogi RODO**, w tym zwiększone obowiązki w zakresie przejrzystości oraz bardziej szczegółowe postanowienia dotyczące praw osób, których dane dotyczą, a także powiadamiania o naruszeniu ochrony danych oraz zasad dalszego przekazywania danych.
- W przypadku przekazywania danych przez administratorów do podmiotów przetwarzających lub od podmiotów przetwarzających do subprocesorów, **wymogi art. 28 RODO** zostały uwzględnione w treści SCC. Przedsiębiorcy nie muszą zatem podpisywać osobnej umowy, aby zachować zgodność z art. 28 RODO.
- Klauzule wdrażające wyrok Trybunału Sprawiedliwości UE w sprawie *Schrems II*: strony SCC muszą obecnie przeprowadzić **"ocenę skutków przekazania danych"**, dokumentując konkretne okoliczności ich przekazania, przepisy prawa w kraju przeznaczenia oraz dodatkowe zabezpieczenia wprowadzone w celu ochrony danych osobowych.
- **Nowe obowiązki w przypadku dostępu organów publicznych do przekazywanych danych**, np.
  obowiązek udzielania informacji podmiotom przekazującym dane oraz obowiązek zaskarżania niezgodnych z prawem żądań dostępu do danych.

22. Czy podmioty przekazujące i podmioty odbierające dane, które nadal stosują "stare" SCC (przyjęte na mocy dyrektywy o ochronie danych z 1995 r.), są zobowiązane do przejścia na nowe SCC (przyjęte w 2021 r.)?

Umowy o przekazywaniu danych do państw trzecich zawarte po 27 września 2021 r., muszą być oparte na nowych SCC.

Podmioty, które zawarły umowę o przekazaniu danych na podstawie poprzednich SCC przed 27 września 2021 r., mogą skorzystać z okresu przejściowego, tj. do 27 grudnia 2022 r., aby wdrożyć nowe SCC (tj. zastąpienie poprzednich SCC, nowymi SCC, wraz z załącznikami). Jeśli operacje przetwarzania danych, które są uregulowane umową opartą treści na poprzednich SCC, ulegną zmianie przed 27 grudnia 2022 r., strony będą już przed tą datą zmuszone, aby przejść na nowe SCC.

Przykład: *podmiot przekazujący dane i podmiot odbierający dane, zawarły umowę o świadczenie usług przed 27 września 2021 r., opierając się na poprzednich SCC. W lutym 2022 r. nastąpiła zmiana cen określonych w umowie o świadczenie usług. Ponieważ zmiana cen nie ma wpływu na* uwarunkowania przekazywania danych osobowych do państw trzecich, *zmiana ta nie wymaga od stron przejścia na nowe SCC (choć nadal należy wdrożyć nowe SCC do 27 grudnia 2022 r.).*

Przykład: *podmiot przekazujący dane i podmiot odbierający dane zawarły umowę o świadczenie usług przed 27 września 2021 r., opierając się na poprzednich SCC. W lutym 2022 r. strony uzgadniają, że przekazywane będą dodatkowe kategorie danych. Zmiana ta ma wpływ na okoliczności przetwarzania danych osobowych, w związku z czym strony muszą przejść na nowe SCC.*

Po 27 XII 2022 r. nie będzie już można opierać transferu na poprzednich SCC.

ZAKRES ZASTOSOWANIA I SCENARIUSZE TRANSFERU

23. Do jakich transferów można wykorzystać SCC?

SCC mogą być wykorzystywane przez administratorów lub podmioty przetwarzające, którzy podlegają reżimowi RODO, do przekazywania danych osobowych administratorom lub podmiotom przetwarzającym działającym poza EOG, którzy nie podlegają RODO.

Po pierwsze, SCC mogą być wykorzystywane przez administratorów i podmioty przetwarzające w EOG, w celu przekazania danych poza EOG, w szczególności gdy planowane jest:

- przekazanie danych osobowych przez administratora działającego w EOG - do administratora lub podmiotu przetwarzającego działającego poza EOG, który nie podlega reżimowi RODO;
- przez podmiot przetwarzający działający w EOG – w celu przekazania danych osobowych dalszemu podmiotowi przetwarzającemu lub administratorowi działającemu poza EOG (w imieniu którego przekazujący podmiot przetwarzający przetwarza dane), który nie podlega reżimowi RODO.

Przykład: *czeska firma wykorzystuje SCC, do przekazywania danych swoich pracowników, do dostawcy usług outsourcingu kadrowego w Singapurze.*

Po drugie, unijne przepisy o ochronie danych mają w określonych sytuacjach bezpośrednie zastosowanie do działalności administratorów i podmiotów przetwarzających funkcjonujących poza EOG, np. z tego względu, iż działają na rynku EOG, oferując towary lub usługi osobom fizycznym w EOG (więcej informacji - patrz: wytyczne Europejskiej Rady Ochrony Danych, dostępne pod adresem https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf). Z uwagi na powyższe, SCC mogą być wykorzystywane przez **administratorów i podmioty przetwarzające działające poza EOG, w celu transferu danych do innych administratorów i podmiotów działających poza EOG**, w szczególności w sytuacji:

- gdy administrator działa poza EOG, ale podejmowane przez niego przetwarzanie podlega reżimowi RODO – zamierza przekazać dane innemu administratorowi lub podmiotowi przetwarzającemu, który również działa poza EOG, ale nie podlega reżimowi RODO;

- gdy podmiot przetwarzający działa poza EOG, ale podejmowane przez niego przetwarzanie podlega reżimowi RODO – zamierza przekazać dane dalszemu podmiotowi przetwarzającemu lub administratorowi, który również działa poza EOG, ale nie podlega reżimowi RODO.

Przykład: *biuro podróży w Tajlandii podlega bezpośrednio reżimowi RODO na mocy jego art. 3 ust. 2, ponieważ oferuje pakiety turystyczne skierowane do klientów europejskich (oferta pakietów jest sporządzana w językach używanych w EOG, dostosowana do potrzeb i preferencji turystów europejskich, z możliwością zapłaty w euro lub innej walucie używanej w EOG itp.). Aby zorganizować zakwaterowanie w Tajlandii, biuro posiada stałą umowę z lokalnym tajlandzkim hotelem. Tajlandzkie biuro podróży może korzystać z SCC (Moduł 1), aby udostępnić tajlandzkiemu hotelowi dane osobowe turystów europejskich.*

24. Czy SCC mogą być wykorzystywane, aby przekazać dane administratorom lub podmiotom przetwarzającym, które podejmują operacje przetwarzania podlegające bezpośrednio RODO?

Nie. (zob. art. 1 decyzji (UE) 2021/914)[3]. SCC zapewniają kompleksowe ramy ochrony danych, opracowane w celu zapewnienia ciągłości ochrony danych, w przypadku przesyłania danych do podmiotów odbierających dane, które nie podlegają RODO.

SCC nie są opracowane dla podmiotów odbierających dane, których operacje przetwarzania podlegają bezpośrednio RODO (zgodnie z art. 3), ponieważ w takim przypadku SCC powielałyby i częściowo modyfikowały obowiązki, które wynikają już bezpośrednio z RODO. **Komisja Europejska jest w trakcie opracowywania dodatkowego zestawu SCC dla takiego scenariusza**, tj. przekazywania danych pomiędzy administratorami i podmiotami przetwarzającymi, którzy bezpośrednio podlegają RODO.

25. Czy SCC mogą być wykorzystane do przekazywania danych osobowych do organizacji międzynarodowej?

SCC zostały opracowane dla podmiotów prywatnych prowadzących działalność komercyjną i **nie są przystosowane do przekazywania danych organizacjom międzynarodowym**. Dla przykładu - organizacje międzynarodowe, które korzystają ze szczególnych przywilejów i immunitetów (np. wynikających z umów międzynarodowych lub porozumień dotyczących siedziby głównej), mogą nie mieć możliwości, aby uznać jurysdykcję organu nadzorczego lub sądu w EOG. Z tego względu do transferów do organizacji międzynarodowej, należy zastosować inne instrumenty, które uwzględniają status organizacji międzynarodowych, np. dostosowane umowy lub porozumienia administracyjne zatwierdzone przez organy nadzorcze. Ponadto, Komisja Europejska jest w trakcie opracowywania SCC, które będą mogły być wykorzystywane przez dostawców usług do przekazywania danych organizacjom międzynarodowym.

26. Czy SCC można wykorzystywać tylko do międzynarodowego przekazywania danych w ramach RODO?

SCC z EOG zostały zatwierdzone przez kilka innych jurysdykcji, jako mechanizm przekazywania danych (np. Zjednoczone Królestwo[4] i Szwajcaria[5]). Zatwierdzenie takie nastąpiło w ramach krajowych przepisów o ochronie danych, przy ograniczonym, formalnym dostosowaniu SCC do krajowego porządku prawnego. Może to znacznie ułatwić przestrzeganie obowiązujących przepisów, zarówno firmom działającym, jak i w tych jurysdykcjach.

Niektóre państwa opracowały **wzorcowe klauzule, które mają wiele cech wspólnych** z europejskimi SCC. Takie klauzule zostały opracowane zarówno na poziomie krajowym (np. Nowa Zelandia[6], Argentyna[7]), jak i w ramach organizacji regionalnych (np. klauzule przyjęte

[3] Decyzja wykonawcza Komisji (UE) 2021/914 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych przy przekazywaniu danych osobowych do państw trzecich na podstawie Rozporządzenia Parlamentu Europejskiego (UE) 2016/679 i Rady.

[4] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/

[5] https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html

[6] https://privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand

[7] https://www.redipd.org/sites/default/files/2021-11/red-iberoamericana-clausulas-contractuales-2021.pdf

przez Iberoamerykańską Sieć Ochrony Danych[8]i Stowarzyszenie Narodów Azji Południowo-Wschodniej[9]). Prace nad wzorcowymi klauzulami dotyczącymi przekazywania danych za granicę toczą się także w ramach Komitetu Konsultacyjnego Konwencji nr 108 Rady Europy.

27. Jakie są dostępne moduły i jak należy wybrać moduł właściwy?

W SCC połączono **klauzule ogólne,** które mają zastosowanie we każdym przypadku (np. sekcja I) wraz z **czterema modułami,** które są dostosowane do różnych scenariuszy transferu danych poza EOG. **Strony muszą wybrać moduł**, **który odpowiada zaistniałemu stanowi faktycznemu,** w szczególności w świetle pełnionych ról, tj. czy są administratorami, podmiotami przetwarzającymi czy subprocesorami (w odniesieniu do znaczenia tych pojęć zob. również wytyczne Europejskiej Rady Ochrony Danych, dostępne tu: https://edpb.europa.eu/our-work-tools/ourdocuments/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

Moduł 1 ma zastosowanie do przekazywania danych przez **administratora** (podmiotu przekazującego dane) do innego **administratora** (podmiotu odbierającego dane).

Przykład: *szwedzkie biuro podróży zawarło umowę ramową z siecią hoteli na organizowanie zakwaterowania dla turystów europejskich na całym świecie. Aby przekazać dane gości do centrum rezerwacji sieci (podmiot odbierający dane) w oparciu o SCC, agencja szwedzka (podmiot przekazujący dane) powinna skorzystać z Modułu 1.*

Moduł 2 ma zastosowanie do przekazywania danych przez **administratora** (podmiotu przekazującego dane) do **podmiotu przetwarzającego** (podmiotu odbierającego dane).

Przykład: *firma w Holandii zleca usługi kadrowe dostawcy działającemu w Indiach. Firma z Holandii powinna skorzystać z Modułu 2, aby przekazać dane swoich pracowników indyjskiemu dostawcy (podmiotowi odbierającemu dane) w oparciu o SCC.*

Moduł 3 dotyczy przekazywania danych przez podmiot przetwarzający (podmiot przekazujący dane) do subprocesora (podmiot odbierający dane).

Przykład: *szpital w Niemczech przekazuje próbki krwi, do analizy w laboratorium w Polsce. Polskie laboratorium zleca niektóre z obszarów swoich usług - indonezyjskiemu instytutowi, specjalizującemu się w analizie genetycznej, wykorzystując w tym celu SCC. Polskie laboratorium (podmiot przekazujący dane) może skorzystać z Modułu 3, aby przekazać dane do indonezyjskiego instytutu (podmiot odbierający dane).*

Moduł 4 dotyczy przekazywania danych przez podmiot przetwarzający (podmiot przekazujący dane) do administratora (podmiot odbierający dane).

[8] https://www.redipd.org/sites/default/files/2021-11/red-iberoamericana-clausulas-contractuales- 2021.pdf

[9] https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data- Flows_Final.pdf.

Przykład 1: firma marokańska korzysta z usług w chmurze oferowanych przez firmę luksemburską w celu zarządzania swoją bazą klientów. SCC (moduł 4) mogą być używane przez przedsiębiorstwo luksemburskie (podmiot przekazujący dane) w celu przesyłania danych ze swojego serwera w Luksemburgu (z powrotem) do klienta w Maroku (podmiot odbierający dane).

Przykład 2: uniwersytet w Tunezji wynajmuje instytut badawczy w Belgii, w celu przeprowadzenia ankiety, w ramach której belgijski instytut zbiera i przetwarza dane w UE, aby następnie przesłać dane na tunezyjską uczelnię. SCC (moduł 4) może być wykorzystany przez instytut belgijski (podmiot przekazujący dane) do przekazywania danych do uniwersytetu w Tunezji (podmiot odbierający dane).

28. Czy kilka modułów może być zastosowanych przez te same strony w tym samym czasie?

Tak. Jak wyjaśniono w odpowiedzi na pytanie 26, strony muszą wybrać moduł(y) odpowiadający(e) zaistniałemu stanowi faktycznemu. **Może się zdarzyć, że strony będą pełnić różne role** w odniesieniu do różnych transferów danych, odbywających się między nimi w ramach łączącego ich stosunku umownego. W takim przypadku **strony powinny skorzystać z odpowiedniego modułu,** dla każdego transferu danych. Na przykład, w przypadku niektórych transferów danych dokonywanych przez administratora (podmiot przekazujący dane), podmiot odbierający dane może działać jako administrator, podczas gdy w przypadku innych transferów, może być podmiotem przetwarzającym. W takim przypadku strony mogą stosować zarówno Moduł 1 (dla tych transferów, dla których zarówno podmiot przekazujący dane, jak i podmiot odbierający dane działają jako administratorzy danych), jak i Moduł 2 (dla tych transferów, dla których podmiot przekazujący dane działa jako administrator, a podmiot odbierający dane jako podmiot przetwarzający).

29. W jaki sposób można zapewnić zgodność z art. 28 RODO?

Wymogi art. 28 RODO zostały włączone do Modułu 2 (przekazywanie danych przez administratora do podmiotu przetwarzającego) i Modułu 3 (przekazywanie danych między podmiotami przetwarzającymi) SCC. W przypadku zastosowania tych modułów, nie jest konieczne zawarcie odrębnej umowy powierzenia przetwarzania, ponieważ moduły niniejsze mogą zapewnić zgodność zarówno z wymogami art. 28 RODO, jak i wymogami związanymi z międzynarodowym transferem danych (art. 46 RODO).

Może również wystąpić sytuacja, w której SCC dotyczące transferu danych są zbędne, ponieważ dostępny jest inny instrument, np. odbiorca danych znajduje się w kraju, wobec którego wydano decyzję stwierdzającą odpowiedni stopień ochrony. W takim przypadku możliwe jest skorzystanie z SCC, aby zapewnić zgodność z art. 28 RODO.

30. W jakich sytuacjach należy zastosować moduł 4 (przekazanie danych przez podmiot przetwarzający dane do administratora)?

Moduł 4 powinien być stosowany, gdy **podmiot przetwarzający funkcjonujący w EOG** działa na rzecz **administratora funkcjonującego poza EOG,** poprzez gromadzenie danych w EOG w imieniu administratora, lub do przetwarzanie w EOG danych otrzymanych od administratora. W tych przypadkach SCC mogą być wykorzystywane przez podmiot przetwarzający, w celu przekazywania danych (bądź przekazywania ich z powrotem) do administratora.

Przykład: *firma marokańska korzysta z usług chmurowych oferowanych przez firmę luksemburską, usługi te polegają na przechowywaniu danych klientów firmy marokańskiej. SCC (Moduł 4) można wykorzystać do transferu danych z Luksemburga (przez podmiot przekazujący dane) (z powrotem) do Maroka (do podmiotu odbierającego dane).*

Przykład: *chilijska firma zleca hiszpańskiemu usługodawcy przeprowadzenie badań rynku i opracowanie materiałów marketingowych, z wykorzystaniem danych klientów otrzymanych z chilijskiej centrali oraz danych klientów zgromadzonych w Hiszpanii. Moduł 4 SCC może być wykorzystywany przez hiszpańskiego usługodawcę do przekazywania do Chile zagregowanych danych dotyczących niniejszych dwóch grup klientów.*

PRAWA OSÓB FIZYCZNYCH W PRZYPADKU TRANSFERU DANYCH NA PODSTAWIE SCC

31. Skąd mogę uzyskać informację, że moje dane są przekazywane poza Europę na podstawie SCC?

Informacja o przekazaniu Twoich danych poza EOG powinna być przekazana przez podmiot przekazujący dane. Artykuły 13 i 14 RODO zobowiązują podmioty przekazujące dany, aby informowały osobę, której dane dotyczą, o zamiarze przekazania danych osobowych poza EOG. **W przypadku zastosowania klauzul SCC, należy również o tym poinformować osobę i wyjaśnić, w jaki sposób można uzyskać kopię** niniejszych klauzul.

W przypadku zastosowania SCC, **podmiot odbierający dane funkcjonujący poza EOG może być również zobowiązany, do przekazania osobom pewnych informacji** (np. swoich danych kontaktowych, kategorii danych osobowych, które przetwarza, oraz odbiorców, którym dane mogą być udostępniane - zob. Moduł 1, klauzula 8.2(a) SCC). Sytuacja taka ma miejsce, gdy podmiot odbierający dane będzie wykorzystywał otrzymane dane do własnych celów (tj. celów innych niż te, dla których dane były przetwarzane przez podmiot przekazujący dane).

32. Zostałem poinformowany, że moje dane zostały przekazane poza EOG w oparciu o SCC. W jaki sposób mogę uzyskać więcej informacji na temat

transferu danych, moich praw, oraz obowiązujących zabezpieczeń? Czy mogę otrzymać kopię treści SCC?

Zgodnie z postanowieniami SCC, strony są zobowiązane do **bezpłatnego** dostarczenia, na żądanie, **kopii** klauzul - w takiej formie, w jakiej zostały **zastosowane**. Dotyczy to wybranych modułów/opcji, a także wypełnionych i podpisanych załączników (w których strony wskazują szczegóły dotyczące przekazywania danych oraz określonych środków, podjętych w celu ochrony danych podczas ich przetwarzania przez podmiot odbierający dane). **Generalne odniesienie do treści SCC** w formie przyjętej przez Komisję Europejską (np. poprzez umieszczenie linku do strony internetowej Komisji) **nie jest wystarczające** (zob. Moduł 1, punkt 8.2 SCC; Moduł 2, punkt 8.3 i Moduł 4, punkt 8.3). Udostępniając Ci kopię klauzul, strony **mogą pominąć jedynie te informacje,** które objęte są tajemnicą handlową lub stanowią inne informacje poufne (np. dane osobowe innych osób), przy czym w takim wypadku niezbędne jest wyjaśnienie, dlaczego te informacje zostały pominięte. Jeżeli pozostała treść jest zbyt trudna do zrozumienia, strony muszą przedstawić proste i jasne streszczenie pominiętych fragmentów (patrz Moduł 1, Punkt 8.2 SCC; Moduł 2, Punkt 8.3 i Moduł 4, Punkt 8.3).

Ponadto, zgodnie z RODO i SCC, masz **prawo do informacji** (np. na temat danych, **które** są przekazywane, celu przetwarzania, odbiorców, którym Twoje dane zostały lub zostaną udostępnione, oraz prawo do złożenia skargi do organu nadzorczego) **od podmiotu odpowiedzialnego za przetwarzanie Twoich danych** (tj. "administratora "). W szczególności można zwrócić się o informacje na temat przetwarzania danych, w tym transferu danych, do podmiotu przekazującego dane, działającego jako administrator zgodnie z art. 15 RODO.

Jeśli dane zostały przekazane przez administratora, podmiotowi działającemu poza EOG, który wykorzystuje niniejsze dane do własnych celów (tj. jako odrębny "administrator"), podmiot przekazujący dane (administrator), będzie mógł udzielić informacji jedynie na temat własnej działalności (wraz z informacją, że dane zostały przekazane poza EOG). W takim przypadku należy skorzystać z prawa do uzyskania informacji bezpośrednio od administratora (podmiotu odbierającego dane) działającego poza EOG, na podstawie zawartych SCC (Moduł 1, Klauzula 10 SCC).

Jeżeli kilka podmiotów jest zaangażowanych w przetwarzanie danych osobowych i nie wiadomo, kto jest administratorem, można skontaktować się z (1) podmiotem, **który przekazał dane osobowe** lub (2) podmiotem **spoza Europy, który otrzymał dane osobowe**. Jeśli podmiot, do którego się zwróciłeś, nie jest w stanie odpowiedzieć Ci bezpośrednio, ponieważ działa jedynie jako dostawca usług (tj. działa w imieniu drugiego podmiotu), SCC wymaga współpracy obu stron w celu rozpatrzenia Twojego wniosku w sposób skuteczny i terminowy.

33. Co zrobić, jeżeli moje dane były przetwarzane z naruszeniem postanowień SCC? Czy mogę uzyskać odszkodowanie? Gdzie można złożyć skargę?

W SCC przewidziano różne sposoby dochodzenia roszczeń, zarówno wobec podmiotu przekazującego, jak i podmiotu odbierającego dane. Pomimo, iż osoba, której dane dotyczą, nie jest stroną SCC, treść SCC umożliwia jej **egzekwowanie klauzul zawierających stosowne**

zabezpieczenia, bezpośrednio wobec stron SCC. W takim przypadku osoba, której dane dotyczą, działa jako beneficjent będący osobą trzecią (zob. klauzula 3 SCC).

Po pierwsze, masz możliwość złożenia skargi bezpośrednio do podmiotu odbierającego dane, który powinien wyznaczyć specjalny punkt kontaktowy do rozpatrywania skarg (zob. klauzula 11 lit. a) SCC). Jeśli podmiot odbierający dane zapewnił możliwość złożenia skargi do niezależnego organu rozstrzygania sporów, można również zwrócić się do tego organu.

Po drugie, masz możliwość złożenia skargi do organu nadzorczego w kraju EOG, w którym mieszkasz. Skargę można wnieść przeciwko podmiotowi odbierającemu dane, jeżeli uważasz, że podmiot ten działał niezgodnie z postanowieniami SCC (zob. klauzula 11 lit. c) SCC), bądź przeciwko podmiotowi przekazującemu dane, jeśli uważasz, podmiot ten przetwarza dane osobowe niezgodnie z prawem (zob. art. 77 RODO).

Po trzecie, możesz wszcząć postępowanie sądowe przeciwko stronom SCC, na przykład w celu uzyskania zabezpieczenia roszczeń lub odszkodowania. Strony SCC ponoszą odpowiedzialność za wszelkie szkody materialne lub niematerialne, które wyrządzą osobie na skutek naruszenia tych postanowień SCC, które zapewniają zabezpieczenia w zakresie przetwarzania danych osobowych lub gwarantują osobom określone prawa (zob. 12 SCC). Powództwo można wnosić do właściwego sądu w kraju EOG (zgodnie z prawem krajowym), w którym mieszka osoba, lub do sądów w EOG, które zostały wskazane przez strony SCC (zob. Klauzula 18(b) i (c) SCC).

Szczególne zasady obowiązują, jeżeli dane zostały przekazane przez dostawcę usług w EOG, który działa w imieniu podmiotu spoza EOG. W takim przypadku masz możliwość złożenia skargi bezpośrednio do podmiotu odbierającego dane (tj. administratora danych działającego poza EOG) lub, jeśli jest to możliwe, do niezależnego organu rozstrzygania sporów (patrz Moduł 4, Klauzula 11). Możesz także zwrócić się do działającego w EOG, podmiotu przekazującego dane, który będzie w tym przypadku musiał współpracować z podmiotem odbierającym dane, w celu rozpatrzenia złożonej skargi (zob. Moduł 4, Klauzula 10). Ponadto, możesz wszcząć postępowanie sądowe przeciwko stronom, w celu uzyskania zabezpieczenia roszczeń lub odszkodowania (zob. Moduł 4, punkt 18, wraz z punktem 3). Takie działania mogą być podejmowane przed sądami wyznaczonymi przez strony SCC.

Wreszcie należy zauważyć, że wspomniane wyżej możliwości uzyskania odszkodowania dotyczą tylko tych praw, które są zapewnione na mocy samych SCC. Niezależnie od tej podstawy, istnieje możliwość uzyskania przez osoby, których dane dotyczą, odszkodowania na podstawie RODO, od podmiotu przekazującego dane. Osoby fizyczne zawsze mają prawo do złożenia skargi do krajowego organu nadzorczego (art. 77 RODO) oraz do uzyskania sądowego środka ochrony prawnej (art. 79 RODO) w związku z przetwarzaniem ich danych przez podmiot przekazujący dane.

OBOWIĄZKI PODMIOTÓW PRZEKAZUJĄCYCH I ODBIERAJĄCYCH DANE

34. Dla Modułów 1, 2 i 3: czy podmiot odbierający dane musi podejmować określone kroki w związku z udostępnianiem otrzymanych danych osobowych stronom trzecim?

Wedle ogólnej zasady, w przypadku, gdy podmiot odbierający dane, dalej udostępnia dane otrzymane na mocy SCC, innemu podmiotowi w kraju lub poza krajem, w którym ma siedzibę, to musi zapewnić, że **nadal wykorzystane będą podobne zabezpieczenia** (zob. Moduł 1, Punkt 8.7; Moduł 2, Punkt 8.8 i Moduł 3, Punkt 8.8). Można tego dokonać na różne sposoby, na przykład poprzez **przystąpienie podmiotu trzeciego do SCC** lub zawarcie **z podmiotem trzecim odrębnej umowy gwarantującej ochronę podobną,** do **ochrony zapewnianej przez SCC**.

W **pewnych szczególnych sytuacjach,** podmiot odbierający dane może udostępniać te dane dalej, także wtedy, gdy nie jest możliwe lub nie jest właściwe uzgodnienie umownych zabezpieczeń ochrony danych z podmiotem trzecim. W szczególności, może być konieczne, aby podmiot odbierający dane, udostępnił niniejsze dane, w **celu ochrony żywotnych interesów osoby, której dane dotyczą,** p.. sieć hoteli musi ujawnić dane gościa hotelowego, lokalnemu szpitalowi, w przypadku nagłej potrzeby medycznej. To samo dotyczy sytuacji, gdy podmiot odbierający dane - musi ujawnić pewne informacje **w ramach krajowego postępowania administracyjnego lub sądowego**, np. firma farmaceutyczna musi udostępnić dane krajowemu organowi regulacyjnemu, aby jej produkty zostały zatwierdzone.

Dodatkowe informacje dla Modułu 1 (administrator danych): jeżeli żadna z powyższych zasad nie ma zastosowania, podmiot odbierający dane może także oprzeć się na wyraźnej zgodzie osób, których dane dotyczą, na dalsze przekazywanie danych podmiotom trzecim (patrz Moduł 1, punkt 8.7(vi)). W takim przypadku podmiot odbierający dane musi upewnić się, że osoba, której dane dotyczą, została poinformowana o celu (celach) przekazania danych, tożsamości podmiotu trzeciego oraz możliwym ryzyku ze względu na brak gwarancji ochrony danych. Podmiot odbierający dane musi również poinformować podmiot przekazujący dane, o dalszym przekazywaniu danych na podstawie zgody. Podmiot przekazujący dane może zażądać kopii informacji, które zostały udostępnione osobie, której dane dotyczą.

35. Czy odpowiedzialność wynikająca z SCC może być ograniczona postanowieniami zawartymi w umowie głównej?

SCC reguluje dwa rodzaje odpowiedzialności: (1) **odpowiedzialność stron wobec osób, których dane dotyczą** (zob. moduł 1 i 4, klauzula 12 lit. b) i c); oraz moduł 2 i 3, klauzula 12 lit. b), c) i e) SCC) oraz (2) **odpowiedzialność między stronami** (zob. Moduł 1 i 4, Klauzula 12(a); oraz Moduł 2 i 3, Klauzula 12(a) SCC). **Postanowienia umowy głównej** (np. dotyczące podziału lub ograniczenia odpowiedzialności) **nie mogą być sprzeczne z zasadami odpowiedzialności wprowadzonymi w SCC** (zob. także Klauzula 2(a) SCC).

Jednocześnie należy zauważyć, że **zasady odpowiedzialności wprowadzone w SCC dotyczą jedynie odpowiedzialności za naruszenie** samych **SCC.** Klauzule dotyczące odpowiedzialności

zawarte w SCC **nie mają wpływu na postanowienia dotyczące odpowiedzialności**, **które mogą mieć zastosowanie do innych aspektów** stosunku umownego zawartego między stronami.

36. Jaki jest wpływ zawarcia SCC na postanowienia umowne między stronami?

Klauzula 16 uprawnia podmiot przekazujący dane do **tymczasowego zawieszenia przekazywania** danych osobowych do podmiotu odbierającego dane, jeżeli ten ostatni narusza klauzule SCC lub nie jest w stanie ich przestrzegać. Ponadto, w pewnych (szczególnie poważnych) przypadkach, podmiot przekazujący dane będzie miał prawo do **rozwiązania** umowy w zakresie, w jakim dotyczy ona przetwarzania danych osobowych. Oznacza to, że prawo do rozwiązania umowy w oparciu o klauzulę 16 jest **ograniczone do tej części umowy, która dotyczy przetwarzania danych osobowych na mocy SCC**.

Jak wyjaśnia klauzula 2 lit. a), strony mogą włączyć SCC do szerszej umowy głównej. Postanowienia **umowy głównej** - a także prawo właściwe dla niej - **będą decydować o tym, czy naruszenie SCC będzie** miało **wpływ na umowę główną,** a w szczególności, czy podmiot przekazujący dane będzie miał prawo do rozwiązania całego stosunku umownego.

Jeżeli operacje przetwarzania danych uregulowane przez SCC dotyczą **więcej niż dwóch stron**, podmiot przekazujący dane może skorzystać z **prawa do rozwiązania umowy tylko względem odpowiedniej strony,** chyba że strony uzgodniły inaczej (zob. klauzula 16 lit. c)).

37. Czy istnieją wymagania dotyczące wyboru prawa właściwego dla umowy?

Klauzula 17 wymaga, aby strony wskazały prawo właściwe do stosowania SCC ("prawo właściwe"). W przypadku **Modułu 1, 2 i 3** musi to być **prawo jednego z państw członkowskich UE lub państw EOG**. W przypadku **Modułu 4** może to być również **prawo kraju, który nie należy do EOG**.

W przypadku wszystkich modułów **właściwym musi być prawo krajowe,** który umożliwia **zastrzeżenie praw na rzecz osób trzecich**. Oznacza to, że wybrane prawo musi zezwalać stronom umowy na zastrzeganie w drodze umowy praw, na które mogą powoływać się zainteresowane osoby, których dane osobowe zostaną przekazane na podstawie SCC.

W przypadku modułów 2 i 3, treść SCC wskazuje, że prawem właściwym będzie co do zasady prawo kraju EOG, w którym podmiot przekazujący dane ma siedzibę, chyba że prawo to nie pozwala na zastrzeganie praw na rzecz osób trzecich (w takim przypadku strony muszą wybrać inne prawo).

Klauzulę 17 **należy interpretować w związku z klauzulą 4**, w której wyjaśniono, że SCC należy interpretować w świetle przepisów RODO - w szczególności tam, gdzie użyto terminów zdefiniowanych w RODO. SCC nie powinny być interpretowane w sposób sprzeczny z prawami i obowiązkami przewidzianymi w RODO. Prawo właściwe, uzgodnione wskazane w klauzuli 17 będzie jednak miało znaczenie, na przykład w przypadku obliczania terminów.

38. Dla Modułu 1, 2 i 3: który organ nadzorczy należy wyznaczyć jako organ właściwy?

Zawierając SCC, **podmiot odbierający dane** wyraża zgodę na **poddanie się jurysdykcji** organu nadzorczego w EOG (klauzula 13). Oznacza to, że podmiot odbierający dane zgadza się współpracować z tym organem we wszelkich procedurach dotyczących zgodności z SCC (np. dochodzeniach, śledztwach i kontrolach) oraz stosować się do decyzji organu nadzorczego w EOG (np. nakazów dostosowania czynności przetwarzania danych do SCC).

Strony powinny wyznaczyć właściwy organ nadzorczy w załączniku I.C do SCC. Jeżeli jest więcej niż jeden podmiot przekazujący dane, właściwych może być kilka organów nadzorczych. Klauzula 13 SCC określa, w jaki sposób wyznaczany będzie organ będzie właściwy.

Jeśli podmiot przekazujący dane ma siedzibę w EOG, wyznaczonym organem nadzorczym powinien być organ właściwy dla podmiotu przekazującego dane. W przypadku przedsiębiorstw prowadzących transgraniczną działalność w zakresie przetwarzania danych w EOG, właściwym będzie wiodący organ nadzorczy.

Jeśli podmiot przekazujący dane nie ma siedziby w EOG, ale podlega bezpośrednio RODO, właściwym organem nadzorczym będzie w zależności od przypadku:

- jeśli podmiot przekazujący dane zobowiązany jest wyznaczyć przedstawiciela (zgodnie z art. 27 RODO): organ nadzorczy w kraju EOG, w którym przedstawiciel ma siedzibę;
- jeśli podmiot przekazujący dane nie ma obowiązku wyznaczyć przedstawiciela (zgodnie z art. 27 RODO): organ nadzorczy w kraju EOG, w którym znajdują się osoby, których dane są przekazywane.

Jednocześnie należy zauważyć, że treść **SCC zezwala osobom, których dane dotyczą, na złożenie skargi** do organu nadzorczego w kraju EOG, w osoby te którym przebywają. Jeżeli jest to inny organ niż ten, który został wyznaczony przez strony, oba organy będą współpracować przy rozpatrywaniu skargi.

39. Czy istnieją wymogi dotyczące wypełniania załączników? Jak szczegółowe powinny być uzupełniane informacje?

Strony muszą wyjaśnić, do **jakich konkretnych** przypadków **transferu danych** zamierzają stosować SCC, w szczególności wskazać kategorie danych osobowych, które są przekazywane, oraz cel (cele), dla których są one przekazywane (załącznik I.A i B). Ponadto strony muszą wskazać swoją **rolę** (jako "podmiot przekazujący dane" lub "podmiot odbierający dane "), także w przypadku późniejszych zmian na podstawie (opcjonalnej) klauzuli dokującej (klauzula 7). Podmioty przekazujące dane, które mają siedzibę poza UE, ale są objęte RODO (art. 3 ust. 2), powinny wskazać swojego przedstawiciela w UE, wyznaczonego zgodnie z art. 27 RODO. Strony muszą również wskazać **właściwy organ lub organy nadzorcze**, zgodnie z klauzulą 13 (załącznik I.C, więcej informacji na temat wyboru właściwego organu znajduje się w odpowiedzi na pytanie 38).

Pomimo, iż w SCC określono ogólne wymagania dotyczące **bezpieczeństwa** danych oraz **przetwarzania danych wrażliwych**, wymagania te należy doprecyzować w odniesieniu do

przedmiotowego przekazywania danych (załącznik I.B i załącznik II). W odniesieniu do bezpieczeństwa, załącznik II zawiera listę przykładów możliwych środków, które można wprowadzić. Strony nie są zobowiązane do wymienienia każdego z tych środków, ale powinny opisać te środki, które są faktycznie wdrażane przez podmiot odbierający dane, w celu zapewnienia odpowiedniego poziomu bezpieczeństwa.

Powyższe szczegółowe informacje, powinny być uzupełnione w Załącznikach, które zgodnie z Klauzulą 1(d), stanowią "integralną część" SCC. Przed wypełnieniem Załączników, strony powinny dokładnie przeanalizować „uwagi wyjaśniające", które znajdują się na pierwszej stronie Załącznika I, oraz na początku Załącznika II.

Przykłady informacji, które należy wskazać w załącznikach (zob. również wytyczne Europejskiej Rady Ochrony Danych, np. dotyczące przejrzystości oraz relacji administrator-przetwarzający.

- Kategorie osób, których dane są przekazywane: np. pracownicy, klienci (osoby fizyczne), osoby będące uczestnikami programu lojalnościowego, osoby fizyczne, które zapisały się do newslettera, dzieci, którym oferowane są usługi społeczeństwa informacyjnego itp.

- Kategorie przekazywanych danych osobowych: np. imię, nazwisko, adres e-mail, numer telefonu, adres miejsca zamieszkania, krajowy numer identyfikacyjny, szczegółowe informacje o płatnościach, informacje dotyczące dokumentacji zdrowotnej itp.

- Cele przekazywania i dalszego przetwarzania danych: wykrywanie działań niezgodnych z prawem, administrowanie listą płac, realizacja płatności bankowych, obsługa klienta, badania rynku itp.

- Charakter przetwarzania: np. przechowywanie, zapisywanie, publikowanie, łączenie, sortowanie, rozpowszechnianie itp.

- Okres, przez który dane będą zatrzymywane, lub kryteria stosowane do określenia tego okresu: konkretny okres może być na przykład określony przez wymogi ustawowe (np. X lat). Jeżeli nie jest możliwe podanie dokładnego okresu, należy wyjaśnić, w jaki sposób zostanie ustalony okres retencji danych, np. na podstawie wytycznych branżowych, czasu obowiązywania umowy powierzenia przetwarzania danych itp. Jeżeli różne kategorie danych osobowych podlegają różnym okresom retencji, każdy okres należy opisać oddzielnie.

40. Czy w przypadku stosowania nowych SCC, konieczne jest podjęcie dodatkowych kroków, w celu zapewnienia zgodności z wyrokiem w sprawie Schrems II? Czy nadal konieczne jest uwzględnianie wskazówek EROD?

Zgodnie z wyrokiem Trybunału Sprawiedliwości UE w sprawie *Schrems II* (C-311/18), **klauzula 14** wymaga od stron, aby przed zawarciem SCC oceniły, czy przepisy i praktyki państwa trzeciego, do którego dane są przekazywane, a mające zastosowanie do przetwarzania danych osobowych przez podmiot odbierający dane, mogłyby uniemożliwić temu podmiotowi przestrzeganie klauzul. Dokonując **"oceny skutków przekazania"**, strony powinny uwzględnić w szczególności okoliczności przekazania (np. kategorie i format danych, rodzaj odbiorcy, sektor gospodarki, w którym następuje przekazanie, oraz długość łańcucha przetwarzania) oraz przepisy i praktyki mające zastosowanie. Ocena skutków przekazania dokonywana jest w celu ustalenia, czy przepisy i obowiązujące praktyki w państwie trzecim, nie wykraczają poza to, co jest konieczne i proporcjonalne w demokratycznym społeczeństwie, do realizacji jednego z celów wymienionych w art. 23 ust. 1 RODO.

Strony **w ramach oceny**, **mogą wziąć pod uwagę różne czynniki** (zob. punkt 14, przypis 12); takie jak wiarygodne informacje na temat stosowania prawa w praktyce (np. orzecznictwo i sprawozdania niezależnych organów), istnienie lub brak żądań organów o ujawnienie informacji w tym samym sektorze oraz, przy spełnieniu ściśle określonych warunków, udokumentowane doświadczenie praktyczne podmiotu przekazującego i/lub odbierającego dane. **W przypadku negatywnej oceny**, strony mogą przekazywać dane na podstawie SCC tylko wówczas, gdy wdrożą **dodatkowe ("uzupełniające") zabezpieczenia** (np. środki techniczne zapewniające bezpieczeństwo danych, takie jak szyfrowanie typu "end-to-end"), które są właściwe dla okoliczności i zapewniają zgodność z klauzulami. To samo dotyczy sytuacji, gdy podmiot przekazujący dane w późniejszym czasie uzyska informację, że podmiot odbierający dane nie jest już w stanie przestrzegać postanowień SCC, także na skutek zmiany przepisów w państwie trzecim. Podmiot przekazujący dane będzie wówczas zobowiązany do wstrzymania przekazywania danych, jeżeli uzna, że nie można zapewnić odpowiednich zabezpieczeń, lub jeżeli otrzyma takie polecenie od właściwego organu nadzorczego.

SCC (Klauzula 14) nie powinny być interpretowane w oderwaniu od innych przepisów, ale **powinny być stosowane wraz ze szczegółowymi wytycznymi przygotowanymi przez Europejską Radę Ochrony Danych (EROD)**. Zob. Zalecenia 01/2020 w sprawie środków uzupełniających narzędzia przekazywania danych w celu zapewnienia zgodności ze stopniem ochrony danych osobowych UE (18 czerwca 2021 r.) (dostępne pod adresem: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf)
.
Zalecenia zawierają mapę drogową działań podejmowanych w ramach oceny, wykaz możliwych źródeł informacji na potrzeby oceny (załącznik 3) oraz przykłady środków uzupełniających (załącznik 2).

41. W jakim zakresie podmiot odbierający dane ma obowiązek informować podmiot przekazujący dane, o żądaniach ujawnienia danych, które otrzymuje od organów publicznych (np. organów ścigania lub organów bezpieczeństwa narodowego)?

Po pierwsze, SCC zawierają **wymóg, aby podmiot odbierający dane, informował o dostępie organów publicznych** do danych, które zostały przekazane.

Zgodnie z klauzulą 15.1, odbierający dane powinien niezwłocznie powiadomić przekazującego dane, jeśli otrzyma od organu publicznego lub sądu w państwie trzecim, **żądanie ujawnienia przekazanych danych osobowych**. Podmiot odbierający dane powinien także poinformować podmiot przekazujący dane, jeśli dowie się o jakimkolwiek **faktycznym dostępie** organów publicznych do takich danych (np. przechwycenie). Treść SCC uwzględnia, iż **prawo krajowe może zakazywać podmiotowi odbierającemu dane** ujawnienia informacji podmiotowi przekazującemu dane, na temat działań organów publicznych. W takim przypadku podmiot odbierający dane powinien dołożyć wszelkich starań, aby uzyskać zwolnienie z niniejszego zakazu, w celu jak najszybszego poinformowania podmiotu przekazującego dane. Jeśli podmiot przekazujący dane sam jest podmiotem przetwarzającym, musi przekazać dalej informację do administratora.

Ponadto **podmiot odbierający dane powinien w regularnych odstępach czasu udostępniać podmiotowi przekazującemu dane, zbiorcze informacje** o otrzymanych żądaniach dostępu (klauzula 15.1(c)). Obowiązek ma zastosowanie tylko wtedy**, gdy podmiot odbierający dane na mocy prawa krajowego jest upoważniony** do przekazywania takich informacji. Jeżeli podmiot przekazujący dane jest jednocześnie podmiotem przetwarzającym, powinien przekazywać te informacje administratorowi.

Po drugie, SCC zawierają **dodatkowe wymogi dotyczące obowiązku powiadamiania w** przypadku, gdy podmiot odbierający dane podlega **przepisom i/lub** praktykom **uniemożliwiającym mu** przestrzeganie klauzul.

Zgodnie z klauzulą 14(e) **podmiot odbierający dane zobowiązuje się do** niezwłocznego **powiadomienia podmiotu przekazującego dane,** jeżeli po zawarciu klauzul, w okresie obowiązywania umowy, będzie miał powody przypuszczać, że **podlega lub zaczął podlegać przepisom lub praktykom niezgodnym z wymaganiami klauzuli 14(a)**. Dotyczy to również sytuacji, gdy przepisy prawa państwa trzeciego ulegną zmianie już po dokonaniu wstępnej oceny lub gdy podmiot odbierający dane będzie podlegał środkom prawnym (np. żądaniu ujawnienia danych) w państwie trzecim, które wskazują na stosowanie w praktyce przepisów w sposób, który nie jest zgodny ze wstępną oceną. Jeśli podmiotem przekazującym dane jest podmiot przetwarzający działający w imieniu administratora, podmiot ten będzie zobowiązany przekazać stosowną informację administratorowi.

Treść SCC uwzględnia **fakt, że podmiot odbierający dane może nie być upoważniony** (na mocy prawa krajowego), do informowania o konkretnych żądaniach dostępu do danych, bądź faktycznego dostępu do danych przez organy publiczne. W szczególności klauzula 16 lit. a) zawiera ogólny wymóg powiadamiania, zgodnie z którym podmiot odbierający dane **musi niezwłocznie poinformować podmiot przekazujący dane,** jeżeli z **jakiegokolwiek powodu nie** jest **w stanie spełnić** wymogów klauzul. Opierając się na tej klauzuli, podmiot odbierający

dane musi poinformować podmiot przekazujący dane, że nie jest w stanie dłużej przestrzegać postanowień SCC, bez konieczności wskazywania konkretnych informacji na temat dostępu organów rządowych do danych. Przekazujący dane będzie mógł wówczas podjąć niezbędne środki, w tym ewentualnie zawiesić przekazywanie danych lub wypowiedzieć SCC.

42. Czy podmiot odbierający dane musi informować osoby, których dane dotyczą, o żądaniach ujawnienia danych otrzymanych od organu publicznego? Co zrobić, jeśli podmiot odbierający dane ma zakaz udzielania takich informacji obowiązujący na mocy prawa krajowego?

Zgodnie z klauzulą 15.1(a), podmiot odbierający dane **musi powiadomić zainteresowane osoby,** w przypadku, gdy otrzyma **żądanie ujawnienia danych osobowych,** od organu publicznego lub sądu w państwie trzecim. Ponadto podmiot odbierający powinien powiadomić podmiot przekazujący dane, jeżeli dowie się o jakimkolwiek **faktycznym dostępie** (np. podsłuchu) organów publicznych do takich danych. Jednocześnie treść **SCC uwzględnia, że przekazanie tych informacji może być niemożliwe ze względów prawnych lub praktycznych.**

W szczególności **podmiot odbierający dane może podlegać zakazowi** (na mocy prawa krajowego), informowania o konkretnych przypadkach dostępu władz publicznych. W takim przypadku podmiot odbierający powinien dołożyć wszelkich starań, aby uzyskać zwolnienie z tego zakazu, mając na celu jak najszybsze przekazanie jak największej ilości informacji.

Ponadto, **w praktyce może zaistnieć trudność, by skontaktować się z osobami**, których dane dotyczą (np. z tego względu, iż podmiot odbierający dane nie ma bezpośredniego kontaktu z tymi osobami). W tej kwestii z klauzuli 15.1(a) wyraźnie wynika, że podmiot odbierający dane może korzystać z pomocy podmiotu przekazującego dane (który może posiadać możliwość bezpośredniego kontaktu z osobami, których dane dotyczą).

43. Czy umowa może zobowiązywać podmiot odbierający dane, do zaskarżania każdego żądania ujawnienia danych, otrzymanego od organu publicznego?

Nie. Zgodnie z klauzulą 15.2 SCC, podmiot odbierający dane **musi zweryfikować**, czy otrzymywane przez niego żądania są zgodne z prawem krajowym. Jeżeli podmiot odbierający **dane** uzna, iż istnieją **uzasadnione podstawy do uznania żądania za niezgodne z prawem** (np. jest oczywiste, że organ występujący z żądaniem przekroczył swoje uprawnienia), podmiot odbierający dane powinien skorzystać z procedur dostępnych w ramach prawa krajowego, w celu zakwestionowania otrzymanego żądania. Jeżeli podmiot odbierający dane zakwestionował żądanie i stoi na stanowisku, iż istnieją **wystarczające podstawy do złożenia odwołania się** od orzeczenia w pierwszej instancji, powinien złożyć takie **odwołanie**.

44. Czy w przypadku korzystania z Modułu 4, konieczne jest przestrzeganie postanowień Sekcji III SCC?

Sekcja III SCC zawiera szczególny wyjątek, w którym moduł 4 jest wykorzystywany przez podmiot **przetwarzający działający w EOG, który dokonuje zwrotu danych do administratora działającego poza EOG, tj. danych które otrzymał od tego administratora**. W tym przypadku dane osobowe, były pierwotnie przetwarzane poza EOG, a więc podlegały już prawu państwa trzeciego. Nie ma zatem potrzeby, aby strony przeprowadzały "ocenę skutków przeniesienia" (klauzula 14) lub wypełniały obowiązki dotyczące dostępu organów publicznych do danych (klauzula 15).

Przykład: *firma marokańska korzysta z usług w chmurze oferowanych przez firmę luksemburską, w celu przechowywania danych zawierających bazę swoich klientów. SCC (Moduł 4) może być wykorzystany w celu przekazywania danych z Luksemburga (przez podmiot przekazujący dane) z powrotem do Maroka. Ponieważ podmiot przekazujący dane odsyła jedynie dane, które wcześniej otrzymał z Maroka, nie musi stosować się do postanowień Sekcji III.*

A contrario, wyjątek ten nie ma zastosowania (a więc strony muszą przestrzegać postanowień Sekcji III), jeżeli dane, które przetwarza podmiot przetwarzający (podmiot przekazujący dane), a następnie przekazuje poza EOG administratorowi (podmiotowi odbierającemu dane), obejmują dane osobowe pochodzące z Europy.

Przykład: *chilijska firma zleca hiszpańskiemu podmiotowi przetwarzającemu, przeprowadzenie badań rynkowych i opracowanie materiałów marketingowych, z wykorzystaniem danych klientów otrzymanych od firmy chilijskiej - oraz danych klientów, które firma hiszpańska zgromadziła w Hiszpanii. Moduł 4 SCC może zostać wykorzystany przez hiszpański podmiot przetwarzający, w celu przekazania do Chile zagregowanych danych, dotyczących tych dwóch zestawów danych. Ponieważ podmiot przekazujący dane przekazuje do podmiotu odbierającego, również dane zebrane w Europie (a nie tylko dane otrzymane z Chile), zobowiązany jest spełnić wymogi sekcji III. Dotyczy to całego zbioru danych przekazywanych do Chile (tj. zarówno danych otrzymanych z Chile, jak i danych zgromadzonych w Hiszpanii).*

PROMOCJA

Dlaczego ODO 24?

Rozwiązania od ludzi dla ludzi

ODO 24 specjalizuje się w ochronie danych osobowych i bezpieczeństwie informacji. Stawiamy na praktyczne i merytoryczne rozwiązania. Wszystko to możemy osiągnąć dzięki trwałym relacjom z klientami, partnerstwu, szacunku i zaufaniu.

ODO 24 w pigułce:

- pomagamy naszym klientom chronić dane i minimalizować ryzyko związane z wyciekiem czy utratą informacji,
- pracujemy w sposób nowoczesny i elastyczny, dostarczając kompleksowe rozwiązania,
- mówimy prostym językiem o skomplikowanych tematach.

Spełniamy najwyższe standardy pracy

CIPM	ISO/IEC 27001	ISO/IEC 29134	ISO/IEC 27701
ISO 31000	ISO/IEC 27005	ISO/IEC 19011	PRINCE2 i SMC™

Wspieramy:

szlachetna PACZKA

AKADEMIA PRZYSZŁOŚCI

POTENCJALNIE NIEBEZPIECZNI

FUNDACJA WIEDZA TO BEZPIECZEŃSTWO

POLSKI CZERWONY KRZYŻ

Zrobimy za Ciebie wszystko to, co zwykle brzmi zawile i niezrozumiale. Wyjaśnimy skomplikowane procesy, wytłumaczymy szczegółowe raporty i pomożemy wdrożyć je w życie.

Maciej Kaczmarski
Prezes zarządu ODO 24

Zapraszam na **naszą stronę**