

# Europejska Rada Ochrony Danych

## Często zadawane pytania dotyczące wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie C-311/18 — Data Protection Commissioner przeciwko Facebook Ireland Ltd i *Maximillianowi Schremsowi*

**Przyjęto 23 lipca 2020 r.**

(tłumaczenie robocze: w przypadku jakichkolwiek wątpliwości ostatecznie rozstrzygającym jest oficjalny tekst dokumentu, dostępny w języku angielskim na stronie Europejskiej Rady Ochrony Danych pod adresem: [https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union\\_en](https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en))

Niniejszy dokument ma na celu przedstawienie odpowiedzi na często zadawane pytania otrzymane przez organy nadzorcze i będzie rozwijany i uzupełniany wraz z dalszymi analizami, biorąc pod uwagę fakt, że EROD nadal analizuje i ocenia wyrok Trybunału Sprawiedliwości Unii Europejskiej (dalej: Trybunał).

Wyrok C-311/18 znajduje się pod linkiem, komunikat prasowy Trybunału znajduje się pod linkiem.

### 1) Co Trybunał orzekł w swoim wyroku?

- ➔ W swoim wyroku Trybunał zbadał ważność decyzji Komisji Europejskiej 2010/87/WE w sprawie standardowych klauzul umownych (SCCs) i uznał ją za ważną. W istocie ważność tej decyzji nie jest podważana przez sam fakt, że standardowe klauzule ochrony danych zawarte w tej decyzji, biorąc pod uwagę ich charakter umowny, nie są wiążące dla organów państwa trzeciego, do którego dane mogą być przekazywane dane.

Trybunał dodał jednak, że ważność ta zależy od tego, czy decyzja 2010/87/WE zawiera skuteczne mechanizmy umożliwiające w praktyce zapewnienie zgodności ze stopniem ochrony merytorycznie równoważnym temu gwarantowanemu w UE przez RODO oraz czy przekazywanie danych osobowych zgodnie z takimi klauzulami jest zawieszane lub zakazane w przypadku naruszenia takich klauzul lub niemożności ich przestrzegania.

W tym względzie Trybunał podkreślił w szczególności, że decyzja 2010/87/WE nakłada na podmiot przekazujący dane i podmiot odbierający dane obowiązek sprawdzenia, przed jakimkolwiek przekazaniem danych, oraz biorąc pod uwagę okoliczności towarzyszących temu przekazywaniu, czy taki stopień ochrony jest przestrzegany w danym państwie trzecim oraz że decyzja 2010/87/WE nakłada na podmiot odbierający dane obowiązek poinformowania podmiotu przekazującego dane o swej ewentualnej niemożności wywiązania się z przestrzegania standardowych klauzul ochrony danych, i w przypadkach w których jest to konieczne, że środków uzupełniających, które są przewidziane w tej klauzuli, wówczas podmiot przekazujący dane będzie z kolei zobowiązany do zawieszenia przekazywania danych czy też rozwiązania umowy z podmiotem odbierającym dane.

- ➔ Trybunał zbadał również ważność decyzji w sprawie Tarczy Prywatności (decyzja 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA), w związku z faktem, że przekazanie danych będące przedmiotem sporu krajowego prowadzącego do wniosku o wydanie orzeczenia w trybie prejudycjalnym, miały miejsce między Unią Europejską a Stanami Zjednoczonymi („USA”).

Trybunał uznał, że wymogi prawa krajowego Stanów Zjednoczonych, a w szczególności niektóre programy umożliwiające amerykańskim władzom publicznym dostęp do danych osobowych przekazywanych z Unii Europejskiej do Stanów Zjednoczonych do celów bezpieczeństwa narodowego, skutkują ograniczeniami w zakresie ochrony danych osobowych, które nie są ograniczone w sposób spełniający wymogi merytorycznie równoważne z wymogami prawa UE<sup>1</sup>, oraz że przepisy te nie przyznają osobom, których dane dotyczą, praw, które mogłyby być egzekwowalne wobec władz amerykańskich przed sądami.

W wyniku takiego stopnia ingerencji w prawa podstawowe osób, których dane są przekazywane do tego państwa trzeciego, Trybunał stwierdził nieważność decyzji w sprawie adekwatności Tarczy Prywatności.

## **2) Czy wyrok Trybunału ma wpływ na inne narzędzia służące do przekazywania danych niż Tarcza Prywatności?**

→ Ogólnie rzecz biorąc, w przypadku państw trzecich próg ustalony przez Trybunał ma również zastosowanie do wszystkich odpowiednich zabezpieczeń na mocy art. 46 RODO stosowanych do przekazywania danych z EOG do dowolnego państwa trzeciego. Prawo Stanów Zjednoczonych, na które powołuje się Trybunał (tj. art. 702 FISA i rozporządzenie wykonawcze nr 12333) ma zastosowanie do każdego przekazywania danych do Stanów Zjednoczonych drogą elektroniczną, objętego zakresem tych przepisów, niezależnie od narzędzia służącego do przekazywania danych<sup>2</sup>.

## **3) Czy istnieje jakiś okres karencji, w którym mogę nadal przysyłać dane do USA bez oceny podstawy prawnej do przekazania danych?**

→ Nie, Trybunał unieważnił decyzję w sprawie Tarczy Prywatności bez utrzymania jej skutków, ponieważ ocenione przez Trybunał prawo Stanów Zjednoczonych nie zapewnia zasadniczo równoważnego stopnia ochrony jak w Unii Europejskiej. Ocenę tę należy wziąć pod uwagę każdorazowo w przypadku przekazywania danych do Stanów Zjednoczonych.

## **4) Przesyłałem dane do amerykańskiego podmiotu odbierającego dane, który przestrzega Tarczy Prywatności, co powinienem teraz zrobić?**

→ Przekazywanie danych na podstawie tych ram prawnych jest nielegalne. Jeśli chcesz nadal przysyłać dane do USA, musisz sprawdzić, czy możesz to zrobić na warunkach określonych poniżej.

## **5) Używam standardowe klauzule umowne z podmiotem odbierającym dane w USA, co powinienem zrobić?**

→ Trybunał stwierdził, że prawo amerykańskie (tj. art. 702 FISA i rozporządzenie wykonawcze 12333) nie zapewnia merytorycznie równoważnego stopnia ochrony.

To, czy możliwe będzie przekazywanie danych osobowych na podstawie standardowych klauzul umownych, zależy będzie od wyniku Twojej oceny, biorąc pod uwagę okoliczności przekazywania oraz środki uzupełniające, które możesz zastosować. Środki uzupełniające, wraz ze standardowymi klauzulami umownymi, po każdorazowej analizie okoliczności towarzyszących przekazywaniu, musiałyby zapewnić, że prawo USA nie ma negatywnego wpływu na odpowiedni stopień ochrony,

---

<sup>1</sup> Trybunał podkreśla, że niektóre programy nadzoru umożliwiające amerykańskim organom publicznym dostęp do danych osobowych przekazywanych z Unii Europejskiej do Stanów Zjednoczonych do celów bezpieczeństwa narodowego nie przewidują żadnych ograniczeń ustanowionego w nim uprawnienia przyznanego władzom USA ani istnienia gwarancji dla osób potencjalnie nimi objętymi spoza USA.

<sup>2</sup> Art. 702 FISA ma zastosowanie do wszystkich "dostawców usług łączności elektronicznej" (zob. definicja w art. 50 Kodeksu Stanów Zjednoczonych § 1881 lit. b) pkt 4), podczas gdy rozporządzenie wykonawcze 12 333 reguluje nadzór elektroniczny, który definiuje się jako "nabycie niepublicznej komunikacji drogą elektroniczną bez zgody osoby będącej stroną łączności elektronicznej lub, w przypadku łączności nieelektronicznej, bez zgody osoby, która jest widoczna w miejscu komunikacji, ale nie obejmuje korzystania ze sprzętu radiowego służącego wyłącznie do określania lokalizacji nadajnika » (3.4 ;b)).

który gwarantują.

Jeśli dojdiesz do wniosku, biorąc pod uwagę okoliczności towarzyszących przekazywaniu oraz możliwe środki dodatkowe, że nie można zapewnić odpowiednich zabezpieczeń, wymagane jest od Ciebie zawieszenie lub zakończenie przekazywania danych osobowych. Jednakże jeśli zamierzasz w dalszym ciągu przekazywać dane pomimo tego wniosku, musisz zgłosić to swojemu właściwemu organowi nadzorcemu<sup>3</sup>.

#### **6) Używam wiążących reguł korporacyjnych („BCR”) z podmiotem w USA; co powinienem/powinnam zrobić?**

- ➔ Biorąc pod uwagę wyrok Trybunału, który unieważnił Tarcza Prywatności z uwagi na stopień ingerencji, jaki stworzyło prawo USA w podstawowe prawa osób, których dane przekazywane są do tego państwa trzeciego oraz fakt, że Tarcza Prywatności została również zaprojektowana by zapewnić gwarancje danym przekazywanym przy wykorzystaniu innych narzędzi, takich jak wiążące reguły korporacyjne, ocena Trybunału ma zastosowanie również w kontekście BCR ze względu na to, że prawo USA będzie miało pierwszeństwo w stosunku do tego narzędzia.

To, czy można przekazywać dane osobowe na podstawie BCR, czy też nie, zależeć będzie od wyniku Twojej oceny przy wzięciu pod uwagę okoliczności towarzyszących przekazywaniu oraz środków uzupełniających, które możesz zastosować. Te środki uzupełniające, wraz z BCR, po każdorazowej analizie okoliczności towarzyszących przekazywaniu, musiałyby zapewnić, że prawo USA nie ma negatywnego wpływu na odpowiedni stopień ochrony, który gwarantują.

Jeśli dojdiesz do wniosku, biorąc pod uwagę okoliczności towarzyszących przekazywaniu oraz możliwe środki uzupełniające, że nie można zapewnić odpowiednich zabezpieczeń, wymagane jest od Ciebie zawieszenie lub zakończenie przekazywania danych osobowych. Jednakże jeśli zamierzasz w dalszym ciągu przekazywać dane pomimo tego wniosku, musisz zgłosić to swojemu właściwemu organowi nadzorcemu<sup>4</sup>.

#### **7) Co z innymi narzędziami przekazywania danych na podstawie art. 46 RODO?**

- ➔ EROD dokona oceny konsekwencji wyroku względem narzędzi innych niż standardowe klauzule umowne oraz wiążące reguły korporacyjne. Wyrok wyjaśnia, że standardem dla odpowiednich zabezpieczeń z art. 46 RODO jest „niezbędna równowaga”.

Jak podkreślił Trybunał, należy zauważyć, że artykuł 46 pojawia się w Rozdziale V RODO i, odpowiednio, musi być odczytywany w świetle art. 44 RODO, który stwierdza, że „wszystkie przepisy niniejszego rozdziału należy stosować z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu”.

#### **8) Czy mogę polegać na wyjątkach z art. 49 RODO by przekazywać dane do USA?**

- ➔ Przekazywanie danych z EOG do USA wciąż jest możliwe na podstawie wyjątków przewidzianych w art. 49 RODO, pod warunkiem, że mają zastosowanie warunki określone w tym artykule. EROD odwołuje się do swoich wytycznych dotyczących tego przepisu<sup>5</sup>.

---

<sup>3</sup> Zob. w szczególności motyw 145 wyroku Trybunału oraz klauzulę 4(g) decyzji Komisji 2010/87/UE, a także klauzulę 5(a) decyzji Komisji 2001/497/WE oraz Zestaw Załączników II (c) decyzji Komisji 2004/915/WE.

<sup>4</sup> Zob. w szczególności motyw 145 wyroku Trybunału oraz klauzulę 4(g) decyzji Komisji 2010/87/UE. Zob. również rozdział 6.3 WP256 rev.01 (Grupa Robocza Art. 29, Dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych, zatwierdzony przez EROD, [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=614109](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109)) oraz rozdział 6.3 WP257 rev.01 (Grupa Robocza Art. 29, Dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych dla podmiotów przetwarzających, zatwierdzony przez EROD, [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=614110](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110)).

<sup>5</sup> Zob. Wytyczne 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679, przyjęte dnia 25 maja 2018 r., [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines\\_2\\_2018\\_derogations\\_pl.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_pl.pdf)

Należy w szczególności przypomnieć, że gdy przekazywanie jest oparte na zgodzie osoby, której dane dotyczą, powinna ona być:

- wyraźna,
- szczegółowa dla konkretnego przekazywania danych lub ich zestawu (co oznacza, że przekazujący dane musi upewnić się, że uzyskał szczegółową zgodę przed przekazaniem danych, nawet jeśli ma to miejsce po zebraniu danych), oraz
- świadoma, szczególnie względem możliwego ryzyka przekazywania (co oznacza, że osoba, której dane dotyczą, powinna być również poinformowana o szczegółowym ryzyku wynikającym z faktu, że jej dane będą przekazane do państwa, które nie zapewnia odpowiedniej ochrony oraz że żadne odpowiednie zabezpieczenia mające na celu zapewnienie ochrony danym nie są wdrażane).

Odnosnie przekazywania niezbędnego dla wykonania umowy między osobą, której dane dotyczą, a administratorem, należy mieć na uwadze, że dane osobowe mogą być przekazywane tylko w przypadku, gdy jest to przekazanie o charakterze sporadycznym. Należałoby ustalać dla każdego przypadku z osobna, czy przekazywanie można byłoby określić jako „sporadyczne” czy „niesporadyczne”. W każdym razie na ten wyjątek można się powoływać tylko wtedy, gdy przekazywanie jest obiektywnie niezbędne do wykonania umowy.

Odnosnie przekazywania niezbędnego z uwagi na ważne względy interesu publicznego (które muszą być zidentyfikowane w prawie UE lub państw członkowskich<sup>6</sup>), EROD przypomina, że zasadniczym wymogiem stosowania tego wyjątku jest stwierdzenie ważnego interesu publicznego, a nie charakter organizacji i że mimo tego, że wyjątek ten nie jest ograniczony do „sporadycznego” przekazywania danych, nie oznacza to, że przekazywanie danych na podstawie wyjątku związanego z ważnym interesem publicznym może odbywać się na dużą skalę i w sposób systematyczny. Należy raczej przestrzegać ogólnej zasady, zgodnie z którą wyjątki określone w art. 49 RODO nie powinny stać się „regułą” w praktyce, ale powinny być ograniczone do określonych sytuacji, a każdy podmiot przekazujący dane musi zapewnić, aby przekazywanie wypełniało test ścisłej konieczności (niezbędności).

#### **9) Czy mogę nadal wykorzystywać standardowe klauzule umowne lub wiążące reguły korporacyjne by przekazywać dane do państwa trzeciego innego niż USA?**

- Trybunał wskazał, że standardowe klauzule umowne co do zasady nadal można wykorzystywać do przekazywania danych do państwa trzeciego, jednak próg ustalony przez Trybunał dla przekazywania danych do USA ma zastosowanie do każdego państwa trzeciego. To samo dotyczy wiążących reguł korporacyjnych.

Trybunał podkreślił, że podmiot przekazujący dane i podmiot odbierający dane są odpowiedzialne za ocenę, czy w danym państwie trzecim przestrzegany jest stopień ochrony wymagany przez prawo UE, aby ustalić, czy gwarancje udzielone przez standardowe klauzule umowne lub wiążące reguły korporacyjne mogą być przestrzegane w praktyce. Jeśli tak nie jest, powinieneś ocenić, czy możesz zapewnić środki uzupełniające, aby zapewnić merytorycznie równoważny stopień ochrony, jaki zapewniany jest w EOG i czy prawo państwa trzeciego nie będzie miało negatywnego wpływu na te środki uzupełniające, zapobiegając ich skuteczności.

Możesz skontaktować się z odbiorcą danych, aby zweryfikować ustawodawstwo jego kraju i współpracować przy jego ocenie. Jeśli Ty lub odbiorca danych w państwie trzecim stwierdzicie, że dane przekazane na podstawie standardowych klauzul umownych lub wiążących reguł korporacyjnych nie są objęte stopniem ochrony zasadniczo równoważnym ze stopniem ochrony gwarantowanym w EOG, należy natychmiast zawiesić przekazywanie. Jeśli tego nie zrobisz, musisz

---

<sup>6</sup> Odniesienia do „państw członkowskich” powinny być rozumiane jako odniesienia do „państw członkowskich EOG”.

powiadomić właściwy organ nadzorczy<sup>7</sup>.

- ➔ Chociaż, jak podkreślił Trybunał, główna odpowiedzialność za samodzielne dokonanie oceny, czy ustawodawstwo państwa trzeciego umożliwia odbiorcy danych przestrzeganie standardowych klauzul ochrony danych lub wiążących reguł korporacyjnych przed przekazaniem danych osobowych do tego państwa trzeciego, spoczywa przede wszystkim na podmiotach przekazujących i odbierających dane, organy nadzorcze będą również odgrywać kluczową rolę przy egzekwowaniu RODO i wydawaniu dalszych decyzji w sprawie przekazywania danych do państw trzecich.

Zgodnie z wezwaniem Trybunału, aby uniknąć rozbieżnych decyzji, organy ochrony danych będą zatem kontynuować prace w ramach EROD w celu zapewnienia spójności, w szczególności jeśli przekazywanie danych do krajów trzecich musi być zabronione.

#### **10) Jakie środki uzupełniające mogę wprowadzić, jeśli korzystam ze standardowych klauzul umownych lub wiążących reguł korporacyjnych w celu przekazywania danych do państw trzecich?**

- ➔ Środki uzupełniające, które można by rozważyć w razie potrzeby, musiałyby być wprowadzane indywidualnie dla każdego przypadku, z uwzględnieniem wszystkich okoliczności przekazania i po dokonaniu oceny prawa państwa trzeciego, w celu sprawdzenia, czy zapewnia ono odpowiedni stopień ochrony.

Trybunał podkreślił, że dokonanie takiej oceny i zapewnienie niezbędnych środków uzupełniających jest podstawowym obowiązkiem przekazującego i odbierającego dane.

EROD analizuje obecnie orzeczenie Trybunału w celu określenia rodzaju dodatkowych środków, które mogłyby zostać wprowadzone dodatkowo do standardowych klauzul umownych lub wiążących reguł korporacyjnych, niezależnie od tego, czy są to środki prawne, techniczne czy organizacyjne, w celu przekazywania danych do państw trzecich, w których standardowe klauzule umowne lub wiążące reguły korporacyjne same w sobie nie zapewnią wystarczającego stopnia gwarancji.

- ➔ EROD dokładniej przeanalizuje, z czego mogłyby się składać środki uzupełniające i dostarczy więcej wskazówek.

#### **11) Korzystam z usług podmiotu przetwarzającego, który przetwarza dane, za które jestem odpowiedzialny jako administrator danych, skąd mam wiedzieć, czy ten podmiot przetwarzający przekazuje dane do Stanów Zjednoczonych lub innego państwa trzeciego?**

- ➔ Umowa, którą administrator zawiera z podmiotem przetwarzającym dane, zgodnie z art. 28 ust. 3 RODO określa, czy przekazywanie danych jest dozwolone, czy też nie (należy pamiętać, że nawet udzielenie dostępu do danych z kraju trzeciego, na przykład dla celów administracyjnych, również stanowi przekazanie danych).
- ➔ Konieczne jest także udzielenie pozwolenia podmiotom przetwarzającym na przekazywanie danych do państw trzecich w przypadku dalszego przetwarzania danych. Należy zwrócić uwagę i zachować ostrożność, ponieważ duża różnorodność rozwiązań informatycznych może wiązać się z przekazywaniem danych osobowych do państwa trzeciego (np. w celu przechowywania lub konserwacji).

---

<sup>7</sup> Zob. w szczególności motyw 145 wyroku Trybunału. W odniesieniu do standardowych klauzul umownych, zob. Klauzula 4 lit. g) decyzji Komisji 2010/87 /UE, a także klauzula 5 lit. a) decyzji Komisji 2001/497/WE i Załącznik zestaw II lit. c) Decyzji Komisji 2004/915/WE. W odniesieniu do wiążących reguł korporacyjnych patrz Rozdział 6.3 Wytocznych WP256 rev.01 (zatwierdzonych przez EROD) i Rozdział 6.3 WP257 rev.01 (zatwierdzonych przez EROD).

**12) Co mogę zrobić, aby nadal korzystać z usług mojego podmiotu przetwarzającego, jeśli umowa podpisana zgodnie z art. 28 ust. 3 RODO wskazuje, że dane mogą być przekazywane do Stanów Zjednoczonych lub do innego państwa trzeciego?**

- ➔ Jeżeli Twoje dane mogą być przekazywane do Stanów Zjednoczonych i nie można zapewnić dodatkowych środków w celu zagwarantowania, że prawo Stanów Zjednoczonych nie narusza zasadniczo równoważnego stopnia ochrony zapewnianego w EOG przez narzędzia przekazywania danych, ani też nie mają zastosowania odstępstwa na mocy art. 49 RODO, jedynym rozwiązaniem jest wynegocjowanie zmiany lub klauzuli uzupełniającej w umowie, w celu zakazania przekazywania danych do Stanów Zjednoczonych. Dane powinny być nie tylko przechowywane, ale również administrowane w innym miejscu niż w Stanach Zjednoczonych.
- ➔ Jeżeli Twoje dane mogą zostać przekazane do innego państwa trzeciego, powinieneś również sprawdzić ustawodawstwo tego kraju, aby sprawdzić, czy jest ono zgodne z wymogami Trybunału oraz z oczekiwanym stopniem ochrony danych osobowych. Jeżeli nie można znaleźć odpowiedniej podstawy do przekazania danych do państwa trzeciego, dane osobowe nie powinny być przekazywane poza terytorium EOG, a wszystkie działania związane z ich przetwarzaniem powinny odbywać się na terytorium EOG.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)