Zbiór Orzeczeń

WYROK TRYBUNAŁU (wielka izba)

z dnia 16 lipca 2020 r.*

Odesłanie prejudycjalne – Ochrona osób fizycznych w zakresie przetwarzania danych osobowych – Karta praw podstawowych Unii Europejskiej – Artykuły 7, 8 i 47 – Rozporządzenie (UE) 2016/679 – Artykuł 2 ust. 2 – Zakres stosowania – Przekazywanie danych osobowych do państw trzecich do celów handlowych – Artykuł 45 – Decyzja Komisji stwierdzająca odpowiedni stopień ochrony – Artykuł 46 – Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń – Artykuł 58 – Uprawnienia organów nadzorczych – Przetwarzanie przekazanych danych przez organy władzy publicznej państwa trzeciego do celów ochrony bezpieczeństwa narodowego – Ocena odpowiedniości stopnia ochrony zapewnianego w tym państwie trzecim – Decyzja 2010/87/UE – Standardowe klauzule ochrony danych osobowych przekazywanych do państw trzecich – Odpowiednie zabezpieczenia zapewniane przez administratora danych – Ważność – Decyzja wykonawcza (UE) 2016/1250 – Adekwatność ochrony zapewnianej przez Tarczę Prywatności UE–USA –Ważność – Skarga wniesiona przez osobę fizyczną, której dane zostały przekazane z Unii Europejskiej do Stanów Zjednoczonych

W sprawie C-311/18

mającej za przedmiot wniosek o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożony przez High Court (wysoki trybunał, Irlandia) postanowieniem z dnia 4 maja 2018 r., które wpłynęło do Trybunału w dniu 9 maja 2018 r., w postępowaniu:

Data Protection Commissioner

przeciwko

Facebook Ireland Ltd,

Maximillian Schrems,

przy udziale:

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

* Język postępowania: angielski.

TRYBUNAŁ (wielka izba),

w składzie: K. Lenaerts, prezes, R. Silva de Lapuerta, wiceprezes, A. Arabadjiev, A. Prechal, M. Vilaras, M. Safjan, S. Rodin, P.G. Xuereb, L.S. Rossi i I. Jarukaitis, prezesi izb, M. Ilešič, T. von Danwitz (sprawozdawca) i D. Šváby, sędziowie,

rzecznik generalny: H. Saugmandsgaard Øe,

sekretarz: C. Strömholm, administratorka,

uwzględniając pisemny etap postępowania i po przeprowadzeniu rozprawy w dniu 9 lipca 2019 r.,

rozważywszy uwagi, które przedstawili:

– w imieniu Data Protection Commissioner – D. Young, solicitor, B. Murray i M. Collins, SC, oraz C. Donnelly, BL,

– w imieniu Facebook Ireland Ltd – P. Gallagher i N. Hyland, SC, A. Mulligan i F. Kieran, BL, oraz P. Nolan, C. Monaghan, C. O'Neill i R. Woulfe, solicitors,

– w imieniu M. Schremsa – H. Hofmann, Rechtsanwalt, E. McCullough, J. Doherty i S. O'Sullivan, SC, oraz G. Rudden, solicitor,

– w imieniu The United States of America – E. Barrington, SC, S. Kingston, BL, S. Barton i B. Walsh, solicitors,

– w imieniu Electronic Privacy Information Centre – S. Lucey, solicitor, G. Gilmore i A. Butler, BL, oraz C. O'Dwyer, SC,

– w imieniu BSA Business Software Alliance Inc. – B. Van Vooren i K. Van Quathem, advocaten,

– w imieniu Digitaleurope – N. Cahill, barrister, J. Cahir, solicitor, oraz M. Cush, SC,

– w imieniu Irlandii – A. Joyce i M. Browne, w charakterze pełnomocników, których wspierał D. Fennelly, BL,

– w imieniu rządu belgijskiego – J.-C. Halleux i P. Cottin, w charakterze pełnomocników,

– w imieniu rządu czeskiego – M. Smolek, J. Vláčil i O. Serdula, a także A. Kasalická, w charakterze pełnomocników,

– w imieniu rządu niemieckiego – J. Möller, D. Klebs i T. Henze, w charakterze pełnomocników,

– w imieniu rządu francuskiego – A.-L. Desjonquères, w charakterze pełnomocnika

– w imieniu rządu niderlandzkiego – C.S. Schillemans, K. Bulterman i M. Noort, w charakterze pełnomocników,

– w imieniu rządu austriackiego – J. Schmoll i G. Kunnert, w charakterze pełnomocników,

– w imieniu rządu polskiego – B. Majczyna, w charakterze pełnomocnika,

– w imieniu rządu portugalskiego – L. Inez Fernandes, A. Pimenta i C. Vieira Guerra, w charakterze pełnomocników,

– w imieniu rządu Zjednoczonego Królestwa – S. Brandon, w charakterze pełnomocnika, którego wspierali J. Holmes, QC, i C. Knight, barrister,

– w imieniu Parlamentu Europejskiego – M.J. Martínez Iglesias i A. Caiola, w charakterze pełnomocników,

– w imieniu Komisji Europejskiej – D. Nardi, H. Krämer i H. Kranenborg, w charakterze pełnomocników,

– w imieniu Europejskiej Rady Ochrony Danych (EROD) – A. Jelinek i K. Behn, w charakterze pełnomocników,

po zapoznaniu się z opinią Rzecznika generalnego na posiedzeniu w dniu 19 grudnia 2019 r.,

wydaje następujący

Wyrok

1 Niniejszy wniosek o wydanie orzeczenia w trybie prejudycjalnym dotyczy zasadniczo:

– wykładni art. 3 ust. 2 tiret pierwsze, art. 25 i 26 oraz art. 28 ust. 3 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. 1995, L 281, s. 31) w świetle art. 4 ust. 2 TUE oraz art. 7, 8 i 47 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą”),

– wykładni i ważności decyzji Komisji 2010/87/UE z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46 Parlamentu Europejskiego i Rady (Dz.U. 2010, L 39, s. 5), zmienionej decyzją wykonawczą Komisji (UE) 2016/2297 z dnia 16 grudnia 2016 r. (Dz.U. 2016, L 344, s. 100) (zwaną dalej „decyzją w sprawie klauzul standardowych”), oraz

– wykładni i ważności decyzji wykonawczej Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. przyjętej na mocy dyrektywy 95/46 Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA (Dz.U. 2016, L 207, s. 1, zwanej dalej „decyzją w sprawie Tarczy Prywatności”).

2 Wniosek ten został złożony w ramach sporu, jaki zaistniał pomiędzy Data Protection Commissioner (komisarzem ds. ochrony danych, Irlandia, zwanym dalej „komisarzem”) a Facebook Ireland Ltd i Maximillianem Schremsem w przedmiocie wniesionej przez niego skargi dotyczącej przekazywania danych osobowych przez Facebook Ireland spółce Facebook Inc. w Stanach Zjednoczonych.

Ramy prawne

Dyrektywa 95/46

3 Artykuł 3 dyrektywy 95/46, zatytułowany „Zakres”, w ust. 2 stanowił:

„Niniejsza dyrektywa nie ma zastosowania do przetwarzania danych osobowych:

– w ramach działalności wykraczającej poza zakres prawa Wspólnoty, jak np. [rodzaje działalności], o których stanowi tytuł V i VI Traktatu o Unii Europejskiej, a w żadnym razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarczą państwa, gdy działalność ta dotyczy spraw związanych z bezpieczeństwem państwa) oraz działalności państwa w obszarach prawa karnego,

– […]”.

4 Artykuł 25 tej dyrektywy stanowił:

„1. Państwa członkowskie zapewniają, aby przekazywanie do państwa trzeciego danych osobowych […] mogło nastąpić tylko wówczas, gdy niezależnie od zgodności z krajowymi przepisami przyjętymi na podstawie innych przepisów niniejszej dyrektywy, dane państwo trzecie zapewni odpowiedni stopień ochrony.

2. Odpowiedni stopień ochrony danych zapewnianej przez państwo trzecie należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych; […]

[…]

6. Komisja może stwierdzić, zgodnie z procedurą określoną w art. 31 ust. 2, że państwo trzecie zapewnia prawidłowy [odpowiedni] stopień ochrony w znaczeniu ust. 2 niniejszego artykułu, co wynika z jego prawa krajowego lub międzynarodowych zobowiązań, jakie państwo to przyjęło, szczególnie po zakończeniu negocjacji określonych w ust. 5, w zakresie ochrony życia prywatnego i podstawowych praw i wolności osób fizycznych.

Państwa członkowskie podejmują środki niezbędne w celu wykonania decyzji Komisji”.

5 Artykuł 26 ust. 2 i 4 tej dyrektywy przewidywał:

„2. Bez uszczerbku dla ust. 1 państwo członkowskie może zezwolić na przekazanie lub przekazywanie danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony w znaczeniu art. 25 ust. 2, jeżeli administrator danych zaleci odpowiednie zabezpieczenia odnośnie do ochrony prywatności oraz podstawowych praw i wolności osoby oraz odnośnie do wykonywania odpowiednich praw; takie środki zabezpieczające mogą w szczególności wynikać z odpowiednich klauzul umownych.

[…]

4. Jeżeli Komisja postanowi, zgodnie z procedurą określoną w art. 31 ust. 2, że określone klauzule umowne zapewniają odpowiednie środki zabezpieczające wymagane w ust. 2, państwa członkowskie podejmą konieczne środki w celu zastosowania się do decyzji Komisji”.

6 Zgodnie z art. 28 ust. 3 tej samej dyrektywy:

„Każdy organ jest w szczególności wyposażony w:

– uprawnienia dochodzeniowe, jak np. prawo dostępu do danych stanowiących przedmiot operacji przetwarzania danych oraz prawo gromadzenia wszelkich informacji potrzebnych do wykonywania jego funkcji nadzorczych,

– skuteczne uprawnienia interwencyjne, jak np. prawo do wyrażania opinii przed przystąpieniem do operacji przetwarzania danych zgodnie z art. 20, oraz zapewnienia odpowiedniej publikacji swoich opinii, zarządzania blokady, usunięcia lub zniszczenia danych, nakładania czasowego lub ostatecznego zakazu przetwarzania danych, ostrzegania lub upominania administratora danych, lub też prawo kierowania sprawy do parlamentów narodowych lub innych instytucji politycznych,

– prawo pozywania w przypadku naruszenia krajowych przepisów przyjętych zgodnie z niniejszą dyrektywą lub powiadomieni[a] organów sądowych o takim naruszeniu.

[…]”.

Rozporządzenie RODO

7 Dyrektywa 95/46 została uchylona i zastąpiona rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnym rozporządzeniem o ochronie danych) (Dz.U. 2016, L 119, s. 1, zwanym dalej „RODO”).

8 Motywy 6, 10, 101, 103, 104, 107–109, 114, 116 i 141 RODO stanowią:

„(6) Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności. Osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych.

[…]

(10) Aby zapewnić wysoki i spójny stopień ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych w Unii, należy zapewnić równorzędny we wszystkich państwach członkowskich stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem takich danych. Należy zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych. Jeżeli chodzi o przetwarzanie danych osobowych w celu wypełnienia obowiązku prawnego, w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, państwa członkowskie powinny móc zachować lub wprowadzić krajowe przepisy doprecyzowujące stosowanie przepisów niniejszego rozporządzenia. Obok ogólnego, horyzontalnego prawa o ochronie danych wdrażającego dyrektywę 95/46/WE państwa członkowskie przyjęły uregulowania sektorowe w dziedzinach wymagających przepisów bardziej szczegółowych. Niniejsze rozporządzenie umożliwia też państwom członkowskim doprecyzowanie jego przepisów, w tym w odniesieniu do przetwarzania szczególnych kategorii

danych osobowych (zwanych dalej »danymi wrażliwymi«). W tym względzie niniejsze rozporządzenie nie wyklucza możliwości określenia w prawie państwa członkowskiego okoliczności dotyczących konkretnych sytuacji związanych z przetwarzaniem danych, w tym dookreślenia warunków, które decydują o zgodności przetwarzania z prawem.

[…]

(101) Przepływ danych osobowych do państw spoza Unii i do organizacji międzynarodowych oraz z takich państw i z takich organizacji jest niezbędnym warunkiem rozwoju handlu międzynarodowego i współpracy międzynarodowej. Wzrost takiego przepływu spowodował nowe wyzwania i problemy w dziedzinie ochrony danych osobowych. Przekazując dane osobowe z Unii administratorom, podmiotom przetwarzającym lub innym odbiorcom w państwach trzecich lub organizacjom międzynarodowym, nie należy jednak obniżać stopnia ochrony osób fizycznych zapewnianego w Unii niniejszym rozporządzeniem, także w przypadkach dalszego przekazywania danych osobowych: z państwa trzeciego lub organizacji międzynarodowej administratorom lub podmiotom przetwarzającym w tym samym lub w innym państwie trzecim lub tej samej lub innej organizacji międzynarodowej. W każdym przypadku przekazywanie danych do państw trzecich i organizacji międzynarodowych może się odbywać wyłącznie w pełnej zgodzie z niniejszym rozporządzeniem. Przekazywanie może mieć miejsce wyłącznie w przypadkach, gdy administrator lub podmiot przetwarzający przestrzegają warunków określonych w przepisach niniejszego rozporządzenia dotyczących przekazywania danych osobowych państwom trzecim lub organizacjom międzynarodowym – z zastrzeżeniem pozostałych przepisów niniejszego rozporządzenia.

[…]

(103) Komisja może stwierdzić ze skutkiem dla całej Unii, że państwo trzecie – lub terytorium, lub określony sektor w państwie trzecim – lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony danych, gwarantując tym samym pewność i jednolitość prawną w całej Unii w odniesieniu do państw trzecich lub organizacji międzynarodowych, które zostały uznane za zapewniające taki stopień ochrony. W takich przypadkach przekazywanie danych osobowych do tego państwa trzeciego lub tej organizacji międzynarodowej może się odbywać bez potrzeby uzyskania dodatkowego zezwolenia. Komisja może także zdecydować, wcześniej informując o tym państwo trzecie lub organizację międzynarodową i przedstawiając im uzasadnienie, o cofnięciu takiej decyzji.

(104) Zgodnie z podstawowymi wartościami, na których opiera się Unia, w szczególności z ochroną praw człowieka, Komisja powinna w swojej ocenie państwa trzeciego lub terytorium, lub określonego sektora w państwie trzecim wziąć pod uwagę sposób, w jaki dane państwo trzecie przestrzega praworządności, dostępu do wymiaru sprawiedliwości oraz międzynarodowych norm i standardów ochrony praw człowieka, jego prawo ogólne i sektorowe, w tym ustawodawstwo dotyczące bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i porządku publicznego, a także prawo karne. Przy przyjmowaniu decyzji stwierdzających odpowiedni stopień ochrony w odniesieniu do terytorium lub określonego sektora w państwie trzecim należy wziąć pod uwagę jasne i obiektywne kryteria, takie jak konkretne czynności przetwarzania, zakres mających zastosowanie standardów prawnych i ustawodawstwo obowiązujące w danym państwie trzecim. Państwo trzecie powinno dawać gwarancje zapewniające odpowiedni stopień ochrony, zasadniczo odpowiadający stopniowi ochrony zapewnianemu w Unii, w szczególności w przypadkach, gdy dane osobowe są przetwarzane w jednym szczególnym sektorze lub większej ich liczbie. Państwo trzecie powinno w szczególności zapewnić skuteczny niezależny nadzór nad ochroną danych oraz powinno przewidzieć mechanizmy współpracy z organami ochrony danych państw członkowskich, a osoby, których dane dotyczą, powinny uzyskać skuteczne i egzekwowalne prawa oraz skuteczne administracyjne i sądowe środki zaskarżenia.

[…]

(107) Komisja może uznać, że państwo trzecie, terytorium lub określony sektor w państwie trzecim, lub organizacja międzynarodowa przestały zapewniać odpowiedni stopień ochrony danych. W związku z tym przekazywanie danych osobowych do tego państwa trzeciego lub tej organizacji międzynarodowej powinno zostać zakazane, chyba że spełnione są wymogi niniejszego rozporządzenia dotyczące przekazywania z zastrzeżeniem odpowiednich zabezpieczeń, w tym wiążących reguł korporacyjnych oraz wyjątków w odniesieniu do szczególnych sytuacji. W takim przypadku należy przewidzieć konsultacje między Komisją a takimi państwami trzecimi lub organizacjami międzynarodowymi. Komisja powinna niezwłocznie poinformować to państwo trzecie lub tę organizację międzynarodową o powodach oraz podjąć z nimi konsultacje w celu rozwiązania sytuacji.

(108) W razie braku stwierdzenia odpowiedniego stopnia ochrony danych administrator lub podmiot przetwarzający powinni zastosować środki rekompensujące brak ochrony danych w państwie trzecim, zapewniając osobie, której dane dotyczą, odpowiednie zabezpieczenia. Takie odpowiednie zabezpieczenia mogą polegać na skorzystaniu z wiążących reguł korporacyjnych, standardowych klauzul ochrony danych przyjętych przez Komisję, standardowych klauzul ochrony danych przyjętych przez organ nadzorczy lub klauzul umownych dopuszczonych przez organ nadzorczy. Zabezpieczenia te powinny zapewniać, by przestrzegane były wymogi ochrony danych oraz prawa osób, których dane dotyczą, takie same jak w przypadku przetwarzania wewnątrzunijnego, w tym zapewniać dostępność egzekwowalnych praw osoby, której dane dotyczą, i skutecznych środków ochrony prawnej – w tym prawa do skutecznych administracyjnych lub sądowych środków zaskarżenia i do żądania odszkodowania – w Unii lub w państwie trzecim. Powinny one dotyczyć w szczególności przestrzegania ogólnych zasad związanych z przetwarzaniem danych osobowych oraz zasad uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych. […]

(109) Możliwość korzystania przez administratora lub podmiot przetwarzający ze standardowych klauzul ochrony danych przyjętych przez Komisję lub organ nadzorczy nie powinna stanowić dla administratora lub podmiotu przetwarzającego przeszkody, by standardowe klauzule ochrony danych włączyć do szerszej umowy, takiej jak umowa między wspomnianym podmiotem przetwarzającym a innym podmiotem przetwarzającym, ani by dodać inne klauzule lub dodatkowe zabezpieczenia, pod warunkiem że nie są one bezpośrednio lub pośrednio sprzeczne ze standardowymi klauzulami umownymi przyjętymi przez Komisję lub organ nadzorczy ani nie naruszają podstawowych praw lub wolności osób, których dane dotyczą. Należy zachęcać administratorów i podmioty przetwarzające, by w drodze zobowiązań umownych przewidywały dodatkowe zabezpieczenia, stanowiące uzupełnienie dla standardowych klauzul ochrony.

[…]

(114) W każdym przypadku, jeżeli Komisja nie podjęła decyzji stwierdzającej odpowiedni stopień ochrony danych w państwie trzecim, administrator lub podmiot przetwarzający powinni zastosować rozwiązania, które pozwolą osobom, których dane dotyczą, dysponować – gdy przekazanie już dojdzie do skutku – egzekwowalnymi i skutecznymi prawami względem przetwarzania ich danych w Unii, tak że osoby te nadal będą mogły korzystać z podstawowych praw i zabezpieczeń.

[…]

(116) Transgraniczne przekazywanie danych osobowych poza Unią może spowodować wzrost ryzyka, że osoby fizyczne nie będą mogły wykonywać prawa do ochrony danych osobowych, w szczególności w celu ochrony przed niezgodnym z prawem wykorzystaniem lub ujawnieniem

tych informacji. Jednocześnie organy nadzorcze mogą uznać, że nie są w stanie rozpatrzyć skargi lub przeprowadzić postępowania w sprawie działalności, która ma miejsce poza granicami ich państwa. Ich starania na rzecz współpracy w kontekście transgranicznym mogą także zostać zakłócone przez niewystarczające uprawnienia prewencyjne lub zaradcze, niespójne systemy prawne oraz przeszkody praktyczne, takie jak ograniczone środki. […]

[…]

(141) Każda osoba, której dane dotyczą, powinna mieć prawo wniesienia skargi do jednego organu nadzorczego oraz prawo do skutecznego środka ochrony prawnej przed sądem, zgodnie z art. 47 Karty praw podstawowych [Unii Europejskiej], w szczególności w państwie członkowskim, w którym ma miejsce zwykłego pobytu, […] jeżeli uzna, że jej prawa wynikające z niniejszego rozporządzenia są naruszane, lub jeżeli organ nadzorczy nie reaguje na skargę, częściowo lub w całości ją odrzuca lub oddala, lub nie podejmuje działania, choć jest to niezbędne do ochrony praw tej osoby. […]".

9 Artykuł 2 ust. 1 i 2 tego rozporządzenia przewiduje:

„1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

2. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:

a) w ramach działalności nieobjętej zakresem [stosowania] prawa Unii;

b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;

c) przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;

d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom".

10 Artykuł 4 omawianego rozporządzenia stanowi:

„Na użytek niniejszego rozporządzenia:

[…]

2) »przetwarzanie« oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

[…]

7) »administrator« oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

8) »podmiot przetwarzający« oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

9) »odbiorca« oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

[…]”.

11 Artykuł 23 tego samego rozporządzenia brzmi następująco:

„1. Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:

a) bezpieczeństwu narodowemu;

b) obronie;

c) bezpieczeństwu publicznemu;

d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;

[…]

2. W szczególności akt prawny, o którym mowa w ust. 1, musi zawierać szczegółowe przepisy przynajmniej – w stosownym przypadku – o:

a) celach przetwarzania lub kategorii przetwarzania;

b) kategoriach danych osobowych;

c) zakresie wprowadzonych ograniczeń;

d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu;

e) określeniu administratora lub kategorii administratorów;

f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania;

g) ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; oraz

h) prawie osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia".

12 W rozdziale V RODO, zatytułowanym „Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych", zostały zawarte art. 44–50 tego rozporządzenia. Zgodnie z art. 44 tego rozporządzenia, zatytułowanym „Ogólna zasada przekazywania":

„Przekazanie danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, następuje tylko, gdy – z zastrzeżeniem innych przepisów niniejszego rozporządzenia – administrator i podmiot przetwarzający spełnią warunki określone w niniejszym rozdziale, w tym warunki dalszego przekazania danych z państwa trzeciego lub przez organizację międzynarodową do innego państwa trzeciego lub innej organizacji międzynarodowej. Wszystkie przepisy niniejszego rozdziału należy stosować z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu".

13 Artykuł 45 tego rozporządzenia, zatytułowany „Przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony", przewiduje w ust. 1–3:

„1. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja stwierdzi, że to państwo trzecie, terytorium lub określony sektor, lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga żadnego specjalnego zezwolenia.

2. Oceniając, czy stopień ochrony jest odpowiedni, Komisja uwzględnia w szczególności następujące elementy:

a) praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie ustawodawstwo – zarówno ogólne, jak i sektorowe – w tym w dziedzinie bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego oraz dostępu organów publicznych do danych osobowych, a także wdrażanie takiego ustawodawstwa, zasady ochrony danych osobowych, zasady dotyczące wykonywania zawodu, środki bezpieczeństwa, w tym zasady dalszego przekazywania danych osobowych do kolejnego państwa trzeciego lub innej organizacji międzynarodowej, których przestrzega się w tym państwie lub w organizacji międzynarodowej, orzecznictwo, a także istnienie skutecznych i egzekwowalnych praw osób, których dane dotyczą, oraz prawa osób, których dane dotyczą, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia;

b) istnienie i skuteczne działanie co najmniej jednego niezależnego organu nadzorczego w państwie trzecim lub w stosunku do organizacji międzynarodowej, mającego obowiązek zapewniać i egzekwować przestrzeganie przepisów o ochronie danych – w tym posiadające[go] odpowiednie uprawnienia do egzekwowania przestrzegania przepisów – pomagać i doradzać osobom, których dane dotyczą, w toku wykonywania przysługujących im praw, a także współpracować z organami nadzorczymi państw członkowskich;

c) międzynarodowe zobowiązania zaciągnięte przez dane państwo trzecie lub daną organizację międzynarodową lub inne obowiązki wynikające z prawnie wiążących konwencji lub instrumentów oraz z udziału w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych.

3. Po dokonaniu oceny, czy stopień ochrony jest odpowiedni, Komisja może w drodze aktu wykonawczego przyjąć decyzję stwierdzającą, że państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony w rozumieniu ust. 2 niniejszego artykułu. W akcie wykonawczym przewiduje się mechanizm okresowego przeglądu – przynajmniej raz na cztery lata – podczas którego uwzględnia się wszelkie mające znaczenie zmiany w państwie trzecim lub organizacji międzynarodowej. W akcie wykonawczym zostaje określony terytorialny i sektorowy zakres jego zastosowania, a gdy ma to zastosowanie, wskazany zostaje organ nadzorczy lub organy nadzorcze, o których mowa w ust. 2 lit. b) niniejszego artykułu. Akt wykonawczy zostaje przyjęty zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2".

14 Artykuł 46 tego rozporządzenia, zatytułowany „Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń", stanowi w ust. 1–3:

„1. W razie braku decyzji na mocy art. 45 ust. 3 administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej.

2. Odpowiednie zabezpieczenia, o których mowa w ust. 1, można zapewnić – bez konieczności uzyskania specjalnego zezwolenia ze strony organu nadzorczego – za pomocą:

a) prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi;

b) wiążących reguł korporacyjnych zgodnie z art. 47;

c) standardowych klauzul ochrony danych przyjętych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2;

d) standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2;

e) zatwierdzonego kodeksu postępowania zgodnie z art. 40 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą; lub

f) zatwierdzonego mechanizmu certyfikacji zgodnie z art. 42 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.

3. Z zastrzeżeniem zezwolenia właściwego organu nadzorczego odpowiednie zabezpieczenia, o których mowa w ust. 1, można także zapewnić w szczególności za pomocą:

a) klauzul umownych między administratorem lub podmiotem przetwarzającym a administratorem, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej; lub

b) postanowień uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą".

15 Artykuł 49 tego rozporządzenia, zatytułowany „Wyjątki w szczególnych sytuacjach”, stanowi:

„1. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w art. 45 ust. 3 lub braku odpowiednich zabezpieczeń określonych w art. 46, w tym wiążących reguł korporacyjnych, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że:

a) osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którym – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę;

b) przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą;

c) przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, któr[ej] dane dotyczą, między administratorem a inną osobą fizyczną lub prawną;

d) przekazanie jest niezbędne ze względu na ważne względy interesu publicznego;

e) przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń;

f) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, któr[ej] dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody; lub

g) przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego.

Jeżeli przekazanie nie może się opierać na art. 45 ani 46, w tym na przepisach dotyczących wiążących reguł korporacyjnych, i nie ma zastosowania żaden z wyjątków mających zastosowanie w szczególnych sytuacjach zgodnie z akapitem pierwszym niniejszego ustępu, przekazanie do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie, gdy przekazanie nie jest powtarzalne, dotyczy tylko ograniczonej liczby osób, których dane dotyczą, jest niezbędne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, wobec których charakteru nadrzędnego nie mają interesy ani prawa i wolności osoby, której dane dotyczą a administrator ocenił wszystkie okoliczności przekazania danych i na podstawie tej oceny zapewnił odpowiednie zabezpieczenia w zakresie ochrony danych osobowych. Administrator informuje organ nadzorczy o przekazaniu. Poza informacjami, o których mowa w art. 13 i 14, administrator podaje osobie, której dane dotyczą, także informacje o przekazaniu i o ważnych prawnie uzasadnionych interesach realizowanych przez niego.

2. Przekazanie na mocy ust. 1 akapit pierwszy lit. g) nie obejmuje całości danych osobowych ani całych kategorii danych osobowych zawartych w rejestrze. Jeżeli rejestr jest dostępny dla osób mających prawnie uzasadniony interes, przekazanie następuje wyłącznie na żądanie tych osób lub gdy mają one być odbiorcami.

3. Ustęp 1 akapit pierwszy lit. a), b), c) oraz ust. 1 akapit drugi nie mają zastosowania do działalności prowadzonej przez organy publiczne w ramach wykonywania przysługujących im uprawnień publicznych.

4. Interes publiczny, o którym mowa w ust. 1 akapit pierwszy lit. d), musi być uznany w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator.

5. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony prawo Unii lub prawo państwa członkowskiego może z uwagi na ważne względy interesu publicznego wyraźnie nakładać ograniczenia na przekazywanie konkretnych kategorii danych osobowych do państwa trzeciego lub organizacji międzynarodowej. Państwa członkowskie powiadamiają Komisję o takich przepisach.

6. Administrator lub podmiot przetwarzający dokumentują ocenę oraz odpowiednie zabezpieczenia, o których mowa w ust. 1 akapit drugi niniejszego artykułu, w rejestrach, o których mowa w art. 30".

16 Zgodnie z art. 51 ust. 1 RODO:

„Każde państwo członkowskie zapewnia, by za monitorowanie stosowania niniejszego rozporządzenia odpowiadał co najmniej jeden niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii (zwany dalej »organem nadzorczym«)".

17 Zgodnie z art. 55 ust. 1 tego rozporządzenia „[k]ażdy organ nadzorczy jest właściwy do wypełniania zadań i wykonywania uprawnień powierzonych mu zgodnie z niniejszym rozporządzeniem na terytorium swojego państwa członkowskiego".

18 Artykuł 57 ust. 1 wspomnianego rozporządzenia przewiduje:

„Bez uszczerbku dla innych zadań określonych na mocy niniejszego rozporządzenia każdy organ nadzorczy na swoim terytorium:

a) monitoruje i egzekwuje stosowanie niniejszego rozporządzenia;

[…]

f) rozpatruje skargi wniesione przez osobę, której dane dotyczą […], w odpowiednim zakresie prowadzi postępowania w przedmiocie tych skarg i w rozsądnym terminie informuje skarżącego o postępach i wynikach tych postępowań, w szczególności jeżeli niezbędne jest dalsze prowadzenie postępowań lub koordynacja działań z innym organem nadzorczym;

[…]".

19 Zgodnie z art. 58 ust. 2 i 4 tego samego rozporządzenia:

„2. Każdemu organowi nadzorczemu przysługują wszystkie następujące uprawnienia naprawcze:

[…]

f) wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;

[…]

j) nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

[…]

4. Wykonywanie uprawnień powierzonych organowi nadzorczemu na mocy niniejszego artykułu podlega odpowiednim zabezpieczeniom – w tym prawu do skutecznego środka ochrony prawnej przed sądem i rzetelnego procesu, określonym w prawie Unii i prawie państwa członkowskiego zgodnie z kartą praw podstawowych".

20 Artykuł 64 ust. 2 RODO stanowi:

„Każdy organ nadzorczy, przewodniczący Europejskiej Rady Ochrony Danych [EROD] lub Komisja mogą wystąpić o przeanalizowanie przez Europejską Radę Ochrony Danych w celu wydania opinii sprawy mającej charakter ogólny lub wywołującej skutki w więcej niż jednym państwie członkowskim, w szczególności jeżeli właściwy organ nadzorczy nie wywiązuje się z obowiązków dotyczących wzajemnej pomocy zgodnie z art. 61 lub wspólnych operacji zgodnie z art. 62".

21 Zgodnie z art. 65 ust. 1 tego rozporządzenia:

„Aby w poszczególnych sytuacjach zapewnić właściwe i spójne stosowanie niniejszego rozporządzenia, Europejska Rada Ochrony Danych przyjmuje w następujących przypadkach wiążące decyzje:

[…]

c) jeżeli właściwy organ nadzorczy nie wystąpił o opinię do Europejskiej Rady Ochrony Danych w przypadkach, o których mowa w art. 64 ust. 1, lub nie zastosował się do opinii Europejskiej Rady Ochrony Danych wydanej zgodnie z art. 64. W takim przypadku organ nadzorczy, którego sprawa dotyczy, lub Komisja mogą zgłosić sprawę Europejskiej Radzie Ochrony Danych".

22 Artykuł 77 tego rozporządzenia, zatytułowany „Prawo do wniesienia skargi do organu nadzorczego", stanowi:

„1. Bez uszczerbku dla innych [skarg] administracyjnych lub środków ochrony prawnej przed sądem każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza niniejsze rozporządzenie.

2. Organ nadzorczy, do którego wniesiono skargę, informuje skarżącego o postępach i efektach rozpatrywania skargi, w tym o możliwości skorzystania z sądowego środka ochrony prawnej na mocy art. 78".

23 Artykuł 78 tego rozporządzenia, zatytułowany „Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu", przewiduje w ust. 1 i 2:

„1. Bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każda osoba fizyczna lub prawna ma prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego jej dotyczącej.

2. Bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli organ nadzorczy właściwy zgodnie z art. 55 i 56 nie rozpatrzył skargi lub nie poinformował osoby, której dane dotyczą, w terminie trzech miesięcy o postępach lub efektach rozpatrywania skargi wniesionej zgodnie z art. 77".

24 Artykuł 94 RODO stanowi:

„1. Dyrektywa [95/46] zostaje uchylona ze skutkiem od dnia 25 maja 2018 r.

2. Odesłania do uchylonej dyrektywy odczytuje się jako odesłania do niniejszego rozporządzenia. Odesłania do Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, ustanowionej w art. 29 dyrektywy [95/46], należy traktować jako odesłania do Europejskiej Rady Ochrony Danych, ustanowionej niniejszym rozporządzeniem".

25 Zgodnie z art. 99 tego rozporządzenia:

„1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po publikacji w *Dzienniku Urzędowym Unii Europejskiej*.

2. Niniejsze rozporządzenie ma zastosowanie od dnia 25 maja 2018 r.".

Decyzja w sprawie klauzul standardowych

26 Motyw 11 decyzji w sprawie klauzul standardowych brzmi następująco:

„Organy nadzorcze państw członkowskich odgrywają kluczową rolę w tym mechanizmie umownym, zapewniając odpowiednią ochronę danych osobowych po przekazaniu. W wyjątkowych przypadkach, jeżeli podmioty przekazujące dane odmawiają poinstruowania podmiotów odbierających dane lub nie są w stanie tego zrobić we właściwy sposób, co wiąże się z bezpośrednim ryzykiem poważnej szkody dla osób, których dane dotyczą, standardowe klauzule umowne powinny umożliwiać organom nadzorczym kontrolę podmiotów odbierających dane i podwykonawców przetwarzania danych [kolejne podmioty przetwarzające] oraz, w stosownych przypadkach, podjęcie decyzji wiążących dla podmiotów odbierających dane i podwykonawców przetwarzania danych [podmiotów przetwarzających]. Organy nadzorcze powinny być uprawnione do zakazania lub zawieszenia operacji przekazania danych lub zbioru takich operacji wykonywanych na podstawie standardowych klauzul umownych w tych wyjątkowych przypadkach, w których ustalono, że przekazanie na podstawie umowy może mieć istotne negatywne skutki w odniesieniu do gwarancji i obowiązków zapewniających odpowiednią ochronę osób, których dane dotyczą".

27 Artykuł 1 tej decyzji stanowi:

„Standardowe klauzule umowne określone w załączniku uważa się za zapewniające odpowiednie gwarancje ochrony prywatności oraz podstawowych praw i wolności osób fizycznych oraz wykonywania odpowiednich praw zgodnie z wymogami art. 26 ust. 2 dyrektywy [95/46]".

28 Zgodnie z art. 2 akapit drugi wspomnianej decyzji „ma [ona] zastosowanie do przekazywania danych osobowych przez administratorów danych prowadzących działalność gospodarczą w Unii Europejskiej do podmiotów odbierających dane prowadzących działalność gospodarczą poza Unią Europejską, którzy działają jedynie jako przetwarzający dane".

29 Artykuł 3 tej samej decyzji stanowi:

„Do celów niniejszej decyzji stosuje się poniższe definicje:

[…]

c) »podmiot przekazujący dane« oznacza administratora danych, który przekazuje dane osobowe;

d) »podmiot odbierający dane« oznacza administratora danych [podmiot przetwarzający] prowadząc[y] działalność gospodarczą w państwie trzecim, który wyraża zgodę na otrzymywanie od podmiotu przekazującego danych osobowych w celu ich przetwarzania w imieniu podmiotu

przekazującego po przekazaniu zgodnie z instrukcjami tego ostatniego i warunkami określonymi w niniejszej decyzji i który nie podlega systemowi państwa trzeciego zapewniającemu odpowiednią ochronę w rozumieniu art. 25 ust. 1 dyrektywy [95/46];

[…]

f) »właściwe prawo o ochronie danych« oznacza prawodawstwo chroniące podstawowe prawa i wolności osób fizycznych, a w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych, właściwe dla administratora danych w państwie członkowskim, w którym podmiot przekazujący dane prowadzi działalność gospodarczą;

[…]".

30 W pierwotnej wersji sprzed wejścia w życie decyzji wykonawczej 2016/2297, art. 4 decyzji 2010/87 stanowił:

„1. Bez uszczerbku dla swoich kompetencji do podejmowania działań w celu zapewnienia zgodności z przepisami prawa krajowego przyjętego na mocy rozdziałów II, III, V i VI dyrektywy [95/46], właściwe organy w państwach członkowskich mogą wykonywać przysługujące im obecnie uprawnienia do zakazania lub zawieszenia przekazywania danych do państw trzecich w celu ochrony osób fizycznych w zakresie przetwarzania ich danych osobowych, w przypadkach, w których:

a) ustalono, że prawo, któremu podlega podmiot odbierający dane lub podwykonawca przetwarzania [kolejny podmiot przetwarzający], nakłada na niego wymagania dotyczące odstępowania od stosowania zasad ochrony danych, które wykraczają poza ograniczenia konieczne w demokratycznym społeczeństwie w rozumieniu art. 13 dyrektywy [95/46], jeżeli wymagania te mogą mieć istotne negatywne skutki dla gwarancji ustanowionych we właściwym prawie o ochronie danych i w standardowych klauzulach umownych;

b) właściwy organ ustalił, że podmiot odbierający dane lub podwykonawca przetwarzania [kolejny podmiot przetwarzający] naruszył standardowe klauzule umowne określone w załączniku; lub

c) istnieje istotne prawdopodobieństwo, że standardowe klauzule umowne zawarte w załączniku nie są lub nie będą przestrzegane, a kontynuowanie przekazywania danych może stworzyć realne zagrożenie wyrządzenia poważnej szkody osobom, których dane dotyczą.

2. Zakaz lub zawieszenie na mocy ust. 1 znosi się po ustaniu powodów wprowadzenia zawieszenia lub zakazu.

3. Państwa członkowskie niezwłocznie powiadamiają Komisję o podjęciu środków na mocy ust. 1 i 2, a Komisja przesyła te informacje pozostałym państwom członkowskim".

31 Motyw 5 decyzji wykonawczej 2016/2297, wydanej w następstwie ogłoszenia wyroku z dnia 6 października 2015 r., Schrems (C-362/14, EU:C:2015:650), ma następujące brzmienie:

„Mutatis mutandis, decyzja w sprawie odpowiedniej ochrony danych osobowych przyjęta przez Komisję na podstawie art. 26 ust. 4 dyrektywy [95/46] jest wiążąca dla wszystkich organów państw członkowskich, do których jest skierowana, w tym ich niezależnych organów nadzorczych, w zakresie, w jakim skutkuje ona uznaniem, że przekazywanie danych odbywające się na podstawie standardowych klauzul umownych ustanowionych w tej decyzji zapewnia wystarczające środki zabezpieczające wymagane przepisem art. 26 ust. 2 tej dyrektywy. Nie uniemożliwia to krajowemu organowi nadzorczemu wykonywania swoich uprawnień w zakresie kontroli przepływów danych, w tym uprawnienia do zawieszenia lub zakazu przekazywania danych osobowych, jeżeli stwierdzi on,

że przekazywanie danych odbywa się z naruszeniem unijnych lub krajowych przepisów o ochronie danych, jak na przykład w przypadku, gdy importer danych nie przestrzega standardowych klauzul umownych".

32 W obecnym brzmieniu, wynikającym z decyzji wykonawczej 2016/2297, art. 4 decyzji w sprawie klauzul standardowych stanowi:

„W przypadku gdy właściwe organy w państwach członkowskich wykonują swoje uprawnienia na podstawie art. 28 ust. 3 dyrektywy [95/46], co prowadzi do zawieszenia lub ostatecznego zakazu przepływu danych do państw trzecich w celu ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych, dane państwo członkowskie bezzwłocznie informuje o tym Komisję, która przekazuje tę informację pozostałym państwom członkowskim".

33 W załączniku do decyzji w sprawie klauzul standardowych, zatytułowanym „Standardowe klauzule umowne (podmioty przetwarzające)", zawartych zostało dwanaście standardowych klauzul umownych. Zgodnie z klauzulą 3 tego załącznika, zatytułowaną „Klauzula na rzecz osoby trzeciej":

„1. Osoba, której dotyczą dane, może żądać od podmiotu przekazującego dane wykonania niniejszej klauzuli, klauzuli 4 lit. b)–i), klauzuli 5 lit. a)–e) oraz lit. g)–j), klauzuli 6 pkt 1 i 2, klauzuli 7, klauzuli 8 pkt 2 i klauzuli 9–12, jako osoba trzecia, na rzecz której zawarto umowę.

2. Osoba, której dotyczą dane, może żądać od podmiotu odbierającego dane wykonania niniejszej klauzuli, klauzuli 5 lit. a)–e) oraz lit. g), klauzuli 6, klauzuli 7, klauzuli 8 pkt 2 i klauzul 9–12 w przypadkach, w których podmiot przekazujący dane przestał istnieć faktycznie lub formalnie. Jeżeli jednak na podstawie umowy lub z mocy prawa podmiot będący jego następcą przejął wszystkie zobowiązania prawne podmiotu przekazującego dane, skutkiem czego przyjął na siebie jego prawa i obowiązki, osoba, której dane dotyczą, może żądać wykonania wymienionych klauzul od tego następcy.

[…]".

34 Zgodnie z brzmieniem klauzuli 4 tego załącznika, zatytułowanej „Obowiązki podmiotu przekazującego dane":

„Podmiot przekazujący dane zgadza się na poniższe warunki i gwarantuje, że:

a) przetwarzanie danych, włącznie z samym ich przekazywaniem, odbywało się i będzie się nadal odbywało zgodnie z odpowiednimi przepisami właściwego prawa o ochronie danych (i w stosownych przypadkach było przedmiotem powiadomienia odpowiednich władz państwa członkowskiego, w którym podmiot przekazujący dane prowadzi działalność gospodarczą) oraz bez naruszenia odpowiednich przepisów tego państwa;

b) nakazał i będzie nakazywał podmiotowi odbierającemu dane podczas całego okresu świadczenia usług przetwarzania danych osobowych przetwarzanie przekazywanych danych osobowych wyłącznie w imieniu podmiotu przekazującego dane oraz zgodnie z właściwym prawem o ochronie danych i z niniejszymi klauzulami;

[…]

f) jeżeli przekazanie obejmuje szczególne kategorie danych, osoba, której dane dotyczą, została poinformowana lub będzie poinformowana przed przekazaniem lub jak najszybciej po przekazaniu o tym, że jej dane mogą być przekazane do państwa trzeciego, które nie zapewnia odpowiedniej ochrony w rozumieniu dyrektywy [95/46];

g) prześle wszelkie zawiadomienia otrzymane od podmiotu odbierającego dane lub podwykonawcy przetwarzania [podmiotu przetwarzającego] na mocy klauzuli 5 lit. b) i klauzuli 8 pkt 3 do organu nadzorczego ds. ochrony danych, jeżeli podmiot przekazujący dane zdecyduje się kontynuować przekazywanie danych lub znieść zawieszenie;

[…]".

35 Klauzula 5 wspomnianego załącznika, zatytułowana „Obowiązki podmiotu odbierającego dane […]", stanowi:

„Podmiot odbierający dane zgadza się na poniższe warunki i gwarantuje, że:

a) będzie przetwarzał dane osobowe wyłącznie w imieniu podmiotu przekazującego dane i zgodnie z jego instrukcjami oraz niniejszymi klauzulami; jeżeli z jakichkolwiek powodów nie może zapewnić takiej zgodności, zgadza się na natychmiastowe poinformowanie podmiotu przekazującego dane o niemożności spełnienia tego warunku, a podmiot przekazujący dane jest w takim przypadku uprawniony do zawieszenia przekazywania danych lub rozwiązania umowy;

b) nie ma powodu, by sądzić, że prawodawstwo mające do niego zastosowanie uniemożliwia mu wypełnianie instrukcji otrzymanych od podmiotu przekazującego dane i jego obowiązków wynikających z umowy oraz że w przypadku zmiany prawodawstwa, która może mieć istotne negatywne skutki dla gwarancji i obowiązków określonych w niniejszych klauzulach, zawiadomi o tym jak najszybciej podmiot przekazujący dane, który w takim przypadku jest uprawniony do zawieszenia przekazywania danych lub rozwiązania umowy;

[…]

d) niezwłocznie powiadomi podmiot przekazujący dane o:
   (i) jakichkolwiek prawnie wiążących wnioskach o ujawnienie danych osobowych ze strony organów ścigania, chyba że powiadomienie o takim wniosku jest zakazane, na przykład na mocy prawa karnego w celu zachowania poufności postępowań prowadzonych przez organy ścigania,
   (ii) jakimkolwiek przypadkowym lub nieupoważnionym dostępie; oraz
   (iii) jakimkolwiek żądaniu otrzymanym bezpośrednio od osób, których dotyczą dane, bez udzielenia odpowiedzi na to żądanie, chyba że został on w inny sposób upoważniony do takiego postępowania;

[…]".

36 Przypis, do którego odsyłacz znajduje się w tytule klauzuli 5, stanowi:

„Obowiązujące wymogi przepisów krajowych mające zastosowanie do podmiotu odbierającego dane, które nie wykraczają poza to, co konieczne w demokratycznym społeczeństwie na podstawie jednego z interesów wymienionych w art. 13 ust. 1 dyrektywy [95/46] (tj. jeżeli stanowią środek konieczny do zabezpieczenia: bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego, zapobiegania przestępstwom lub czynom stanowiącym naruszenie zasad etyki w zawodach regulowanych i ich dochodzenia, wykrywania i ścigania, ważnego interesu ekonomicznego lub finansowego państwa lub ochrony osoby, której dane dotyczą, lub praw i wolności innych osób), nie są sprzeczne ze standardowymi klauzulami umownymi. […]".

37 Klauzula 6 załącznika do decyzji w sprawie klauzul standardowych, zatytułowana „Odpowiedzialność”, przewiduje:

„1. Strony uzgadniają, że każda osoba, której dotyczą dane, która poniosła szkodę w wyniku jakiegokolwiek naruszenia obowiązków, o których mowa w klauzuli 3 lub 11, przez którąkolwiek ze stron lub podwykonawcę przetwarzania [kolejny podmiot przetwarzający], jest uprawniona do uzyskania odszkodowania za poniesioną szkodę od podmiotu przekazującego dane.

2. Jeżeli osoba, której dane dotyczą, nie jest w stanie wystąpić przeciw podmiotowi przekazującemu dane z roszczeniem o odszkodowanie zgodnie z pkt 1, wynikającym z naruszenia przez podmiot odbierający dane lub jego podwykonawcę przetwarzania [podmiot przetwarzający] któregokolwiek z ich obowiązków, o których mowa w klauzuli 3 lub klauzuli 11, ponieważ podmiot przekazujący dane przestał istnieć faktycznie lub formalnie lub stał się niewypłacalny, podmiot odbierający dane zgadza się na wystąpienie przez osobę, której dotyczą dane, z roszczeniem wobec podmiotu odbierającego dane, tak jakby był on podmiotem przekazującym dane […].

[…]”.

38 Klauzula 8 tego załącznika, zatytułowana „Współpraca z organami nadzorczymi”, stanowi w ust. 2:

„Strony uzgadniają, że organ nadzorczy ma prawo do przeprowadzenia kontroli podmiotu odbierającego dane i jakiegokolwiek podwykonawcy przetwarzania [kolejnego podmiotu przetwarzającego], która ma ten sam zakres i podlega tym samym warunkom, jakie miałyby zastosowanie do kontroli podmiotu przekazującego dane na mocy właściwego prawa o ochronie danych”.

39 W klauzuli 9 tegoż załącznika, zatytułowanej „Właściwe prawo”, wyjaśniono, że klauzule podlegają prawu państwa członkowskiego, w którym prowadzi działalność podmiot przekazujący dane.

40 Zgodnie z brzmieniem klauzuli 11 tego samego załącznika, zatytułowanej „Podwykonawstwo przetwarzania danych”:

„1. Podmiot odbierający dane nie podzleca czynności przetwarzania danych wykonywanych w imieniu podmiotu przekazującego dane na podstawie niniejszych klauzul bez uprzedniej pisemnej zgody podmiotu przekazującego dane. Jeżeli podmiot odbierający dane podzleca wykonanie swoich obowiązków w ramach niniejszych klauzul za zgodą podmiotu przekazującego dane, czyni to wyłącznie na podstawie umowy pisemnej z podwykonawcą przetwarzania [kolejnym podmiotem przetwarzającym], która nakłada na podwykonawcę przetwarzania [tego ostatniego] te same obowiązki, jakie spoczywają na podmiocie odbierającym dane w ramach niniejszych klauzul. […]

2. Umowa pisemna zawarta między podmiotem odbierającym dane a podwykonawcą przetwarzania [kolejnym podmiotem przetwarzającym] przed przekazaniem danych osobowych podwykonawcy przetwarzania [kolejnemu podmiotowi przetwarzającemu] obejmuje również klauzulę na rzecz osoby trzeciej, określoną w klauzuli 3, w odniesieniu do przypadków, w których osoba, której dotyczą dane, nie jest w stanie wystąpić z roszczeniem o odszkodowanie, o którym mowa w klauzuli 6 pkt 1 przeciw podmiotowi przekazującemu lub odbierającemu dane, ponieważ przestały one istnieć faktycznie lub formalnie lub stały się niewypłacalne, a żaden podmiot będący następcą nie przejął na podstawie umowy lub z mocy prawa wszystkich zobowiązań prawnych podmiotu przekazującego lub odbierającego dane. Taka odpowiedzialność podwykonawcy przetwarzania [kolejnego podmiotu przetwarzającego] wobec osoby trzeciej jest ograniczona do jego własnych czynności przetwarzania danych na podstawie niniejszych klauzul.

[…]”.

41 Klauzula 12 załącznika do decyzji w sprawie klauzul standardowych, zatytułowana „Obowiązki po zakończeniu usług przetwarzania danych osobowych”, stanowi w ust. 1:

„Strony uzgadniają, że wraz z zakończeniem świadczenia usług przetwarzania danych podmiot odbierający dane i podwykonawca przetwarzania [kolejny podmiot przetwarzający] zwracają podmiotowi przekazującemu dane wszystkie przekazane dane osobowe i ich kopie lub niszczą wszystkie dane osobowe i poświadczają przekazującemu dane, że to uczynili, zgodnie z decyzją przekazującego dane, chyba że przepisy prawa obowiązujące podmiot odbierający dane uniemożliwiają mu zwrot lub zniszczenie wszystkich lub części przekazanych danych osobowych. […]”.

Decyzja w sprawie Tarczy Prywatności

42 Wyrokiem z dnia 6 października 2015 r., Schrems (C-362/14, EU:C:2015:650), Trybunał orzekł nieważność decyzji Komisji 2000/520/WE z dnia 26 lipca 2000 r. przyjętej na mocy dyrektywy 95/46, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach bezpiecznej przystani oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez departament handlu USA (Dz.U. 2000, L 215, s. 7), w której instytucja ta stwierdziła, że to państwo trzecie zapewnia odpowiedni stopień ochrony.

43 W następstwie wydania tego wyroku i przeprowadzenia oceny uregulowań obowiązujących w Stanach Zjednoczonych Komisja wydała decyzję w sprawie Tarczy Prywatności, w której motywie 65 wskazała:

„Komisja oceniła przewidziane w prawie amerykańskim ograniczenia i gwarancje w zakresie dostępu do danych osobowych przekazywanych przez amerykańskie organy publiczne w ramach Tarczy Prywatności [Unia Europejska]–USA i korzystania z tych danych do celów bezpieczeństwa narodowego, egzekwowania prawa i innych celów leżących w interesie publicznym. Ponadto rząd Stanów Zjednoczonych – za pośrednictwem Urzędu Dyrektora Krajowych Służb Wywiadowczych [(Office of the Director of National Intelligence, ODNI)] […] – przekazał Komisji szczegółowe oświadczenia i zobowiązania, które zawarto w załączniku VI do niniejszej decyzji. Na mocy pisma podpisanego przez sekretarza stanu i dołączonego jako załącznik III do niniejszej decyzji rząd Stanów Zjednoczonych zobowiązał się również do utworzenia nowego mechanizmu nadzoru nad przypadkami ingerencji ze względu na bezpieczeństwo narodowe, tj. do powołania Rzecznika ds. Tarczy Prywatności, który jest organem niezależnym od Wspólnoty Wywiadowczej. W oświadczeniu departamentu sprawiedliwości Stanów Zjednoczonych zawartym w załączniku VII do niniejszej decyzji opisano ograniczenia i gwarancje mające zastosowanie do dostępu organów publicznych do danych w celu egzekwowania prawa i w innych celach leżących w interesie publicznym oraz korzystania z tych danych przez organy publiczne. Aby zwiększyć przejrzystości i odzwierciedlić prawny charakter tych zobowiązań, każdy z dokumentów zamieszczonych w wykazie i załączonych do niniejszej decyzji zostanie opublikowany w amerykańskim rejestrze federalnym [*U.S. Federal Register*]”.

44 Przeprowadzona przez Komisję analiza tych ograniczeń i gwarancji została pokrótce przedstawiona w motywach 67–135 decyzji w sprawie Tarczy Prywatności, podczas gdy wyciągnięte przez tę instytucję wnioski dotyczące odpowiedniego stopnia ochrony zapewnianego w ramach Tarczy Prywatności Unia Europejska–USA zostały zawarte w motywach 136–141 tej decyzji.

45 W szczególności motywy 68, 69, 76, 77, 109, 112–116, 120, 136 i 140 tej decyzji stanowią:

„(68) Zgodnie z konstytucją Stanów Zjednoczonych odpowiedzialność za zapewnienie bezpieczeństwa narodowego spoczywa na prezydencie, który pełni funkcję naczelnego wodza i zwierzchnika sił zbrojnych i który jest uprawniony do kształtowania polityki zagranicznej Stanów Zjednoczonych w obszarze wywiadu zagranicznego […]. Choć kongres posiada kompetencje do nakładania ograniczeń i wielokrotnie korzystał z tego uprawnienia, prezydent jest uprawniony do kierowania działalnością Wspólnoty Wywiadowczej Stanów Zjednoczonych w tym obszarze,

w szczególności za pomocą rozporządzeń wykonawczych lub dyrektyw prezydenta. […] Obecnie można wskazać dwa kluczowe instrumenty prawne w tym obszarze: rozporządzenie wykonawcze nr 12333 (»rozporządzenie wykonawcze [*Executive Order*] nr 12333«) i dyrektywę polityczną prezydenta nr 28 [(*Presidential Policy directive 28*, zwaną dalej »PPD-28«)].

(69) W [PPD-28] na operacje w obszarze »rozpoznania radioelektronicznego« nałożono szereg ograniczeń […]. Dyrektywa prezydenta jest wiążąca dla amerykańskich organów wywiadowczych […] i pozostaje w mocy po zmianie administracji Stanów Zjednoczonych. [PPD-28] ma szczególne znaczenie dla osób niebędących obywatelami ani rezydentami amerykańskimi, uwzględniając osoby z UE, których dane dotyczą. […]

[…]

(76) Zasady [określone w PPD-28] odpowiadają zasadzie konieczności i proporcjonalności, mimo że nie mają takiego samego brzmienia [sformułowania prawnego]. […]

(77) Z uwagi na fakt, że wymogi te zostały zawarte w dyrektywie wydanej przez prezydenta, który pełni funkcję dyrektora wykonawczego, są wiążące dla całej Wspólnoty Wywiadowczej i zostały wdrożone w ramach przepisów i procedur agencyjnych przekładających ogólne zasady na konkretne wskazówki dotyczące codziennej działalności. […]

[…]

(109) Natomiast zgodnie z sekcją 702 ustawy o kontroli wywiadu [Foreign Intelligence Surveillance Act (FISA)] sąd ds. inwigilacji obcych wywiadów [United States Foreign Intelligence Surveillance Court (FISC)] nie jest uprawniony do zatwierdzania poszczególnych środków nadzoru; może jednak zatwierdzać programy nadzoru (takie jak PRISM, UPSTREAM) w oparciu o roczne certyfikacje przygotowywane przez prokuratora generalnego [(United States Attorney General)] i dyrektora krajowych służb wywiadowczych [Director of National Intelligence (DNI)]. […] Jak już wskazano, certyfikacje, które mają zostać zatwierdzone przez sąd ds. inwigilacji obcych wywiadów [FISC] nie zawierają żadnych informacji na temat poszczególnych osób, które mają być namierzane – służą one identyfikowaniu kategorii zagranicznych informacji wywiadowczych […]. Choć Sąd ds. Inwigilacji Obcych Wywiadów [(FISC)] nie ocenia – na podstawie uzasadnionego podejrzenia lub innej normy – czy osoby fizyczne są odpowiednio namierzane do celów pozyskiwania zagranicznych informacji wywiadowczych […], zakres kontroli przeprowadzanej przez ten sąd obejmuje również warunek, zgodnie z którym »istotnym celem gromadzenia informacji jest pozyskanie zagranicznych informacji wywiadowczych« […].

[…]

(112) Po pierwsze, w [FISA] przewidziano liczne środki ochrony prawnej dla osób niebędących obywatelami ani rezydentami USA, dzięki którym mogą zakwestionować prowadzenie bezprawnego dozoru elektronicznego […]. Obejmuje to możliwość wytoczenia powództwa cywilnego przez osoby fizyczne o odszkodowanie pieniężne przeciwko Stanom Zjednoczonym, w przypadku gdy informacje na ich temat zostały bezprawnie i umyślnie wykorzystane lub ujawnione […]; pozwania amerykańskich urzędników rządowych działających we własnym imieniu (»pod przykrywką prawa«) o odszkodowanie pieniężne […]; oraz zakwestionowania legalności dozoru (i wystąpienia o ograniczenie rozpowszechniania informacji), w przypadku gdy rząd zamierza wykorzystać lub ujawnić jakiekolwiek informacje uzyskane lub pochodzące z dozoru elektronicznego przeciwko danej osobie w postępowaniu sądowym lub administracyjnym w Stanach Zjednoczonych […].

(113) Po drugie, rząd USA przedstawił Komisji liczne dodatkowe możliwości, z których mogą skorzystać osoby z UE, których dane dotyczą, aby uzyskać ochronę prawną przeciwko urzędnikom rządowym ze względu na bezprawny dostęp administracji rządowej do danych osobowych lub ich bezprawne wykorzystanie przez administrację rządową, w tym rzekomo do celów bezpieczeństwa narodowego […].

(114) Ponadto rząd USA wskazał ustawę o dostępie do informacji publicznej [Freedom of information Act (FOIA)] jako środek, z którego osoby niebędące obywatelami ani rezydentami USA mogą skorzystać, aby uzyskać dostęp do istniejących rejestrów agencji federalnej, w tym jeżeli rejestry te zawierają dane osobowe tej osoby fizycznej […]. Mając na uwadze główny obszar regulowany ustawą o dostępie do informacji publicznej, [(FOIA)] nie daje […] możliwości skorzystania ze środków ochrony prawnej przez osobę fizyczną w przypadku samej ingerencji w dane osobowe, mimo że mogłaby zasadniczo umożliwić osobom fizycznym uzyskanie dostępu do odpowiednich informacji przechowywanych przez krajowe agencje wywiadowcze. […]

(115) Chociaż osoby fizyczne, w tym osoby z UE, których dane dotyczą, mają zatem liczne możliwości dochodzenia roszczeń, jeżeli zostały objęte bezprawnym dozorem (elektronicznym) do celów bezpieczeństwa narodowego, równie oczywiste jest, że nie uwzględniono przynajmniej niektórych podstaw prawnych, na jakie mogą powołać się amerykańskie organy wywiadowcze (np. rozporządzenie wykonawcze […] nr 12333). Co więcej, nawet jeżeli osoby niebędące obywatelami ani rezydentami USA mogą zasadniczo korzystać z sądowych środków odwoławczych, np. w przypadku nadzoru na mocy [FISA], dostępne podstawy wszczęcia powództwa są jednak ograniczone […], a roszczenia zgłaszane przez osoby fizyczne (w tym osoby będące obywatelami lub rezydentami USA) zostaną uznane za niedopuszczalne, jeżeli osoby te nie mogą wykazać interesu prawnego […], co ogranicza dostęp do sądów powszechnych […].

(116) Aby zapewnić dodatkowe możliwości ochrony prawnej dostępne dla wszystkich osób z UE, których dane dotyczą, rząd USA podjął decyzję o utworzeniu nowego urzędu Rzecznika, jak wskazano w piśmie sekretarza stanu USA do Komisji, które znajduje się w załączniku III do niniejszej decyzji. Ten urząd opiera się na wyznaczeniu na podstawie [PPD-28] starszego koordynatora (na poziomie podsekretarza) w departamencie stanu jako osobę odpowiedzialną za kontakty dla rządów zagranicznych, aby mogły one wyrazić obawy dotyczące działań USA w zakresie rozpoznania radioelektronicznego; funkcja ta wykracza jednak daleko poza pierwotny zakres.

[…]

(120) [R]ząd Stanów Zjednoczonych zobowiązuje się do zapewnienia, aby Rzecznik ds. Tarczy Prywatności – pełniąc swoje funkcje – mógł opierać się na współpracy z innymi istniejącymi w prawie amerykańskim mechanizmami niezależnego nadzoru i przeglądu zgodności. […] Jeżeli jeden ze wypomnianych organów nadzorczych stwierdzi jakikolwiek przypadek nieprzestrzegania zasad, jednostka Wspólnoty Wywiadowczej (np. agencja wywiadowcza), której dotyczy ten zarzut, będzie musiała zaradzić takiemu nieprzestrzeganiu zasad, ponieważ tylko w taki sposób Rzecznik będzie mógł udzielić pozytywnej odpowiedzi osobie fizycznej (tj. że zaradzono ewentualnemu nieprzestrzeganiu zasad), do czego zobowiązał się rząd Stanów Zjednoczonych. […]

[…]

(136) W świetle tych ustaleń Komisja uznaje, że Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do samocertyfikowanych podmiotów w Stanach Zjednoczonych w ramach Tarczy Prywatności [Unia Europejska]–USA.

[…]

(140) Ponadto na podstawie dostępnych informacji na temat amerykańskiego porządku prawnego, w tym oświadczeń i zobowiązań rządu USA, Komisja stwierdza, że wszelkie ingerencje amerykańskich organów publicznych w prawa podstawowe osób, których dane osobowe są przekazywane z Unii do Stanów Zjednoczonych w ramach Tarczy Prywatności [Unia Europejska]–USA do celów bezpieczeństwa narodowego, egzekwowania prawa lub innych celów interesu publicznego, a także wiążące się z nimi ograniczenia nałożone na samocertyfikowane podmioty w odniesieniu do przestrzegania przez nie zasad, będą ograniczać się do tego, co jest ściśle niezbędne, aby osiągnąć dany uzasadniony cel, oraz że istnieje skuteczna ochrona prawna przed taką ingerencją".

46 Zgodnie z brzmieniem art. 1 decyzji w sprawie Tarczy Prywatności:

„1. Do celów art. 25 ust. 2 dyrektywy [95/46] Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do podmiotów w Stanach Zjednoczonych w ramach Tarczy Prywatności [Unia Europejska]–USA.

2. Na Tarczę Prywatności [Unia Europejska]–USA składają się zasady wydane przez departament handlu Stanów Zjednoczonych w dniu 7 lipca 2016 r., jak wskazano w załączniku II, oraz oficjalne oświadczenia i zobowiązania zawarte w dokumentach przedstawionych w załącznikach I, III–VII.

3. Do celów ust. 1 dane osobowe są przekazywane w ramach Tarczy Prywatności [Unia Europejska]–USA, w przypadku gdy przekazuje się je z Unii do podmiotów w Stanach Zjednoczonych, które figurują w »wykazie podmiotów uczestniczących w programie Tarczy Prywatności« prowadzonym i udostępnianym publicznie przez departament handlu Stanów Zjednoczonych zgodnie z sekcjami I i III zasad przedstawionych w załączniku II".

47 W pkt I.5 załącznika II do decyzji w sprawie Tarczy Prywatności, zatytułowanego „Ramowe zasady Tarczy Prywatności [Unia Europejska]–USA wydane przez departament handlu Stanów Zjednoczonych", przewidziano, że przyjęcie zasad może być ograniczone w szczególności „w zakresie niezbędnym do spełnienia wymogów bezpieczeństwa narodowego, interesu publicznego lub egzekwowania prawa".

48 Załącznik III do tej decyzji zawiera pismo z dnia 7 lipca 2016 r., skierowane przez Johna Kerry'ego, pełniącego wówczas funkcję Secretary of State (sekretarza stanu, Stany Zjednoczone), do [unijnego] komisarza ds. sprawiedliwości, konsumentów i równouprawnienia płci, do którego w załączniku A załączono memorandum zatytułowane „Urząd Rzecznika ds. Tarczy Prywatności [Unia Europejska]–USA w odniesieniu do rozpoznania radioelektronicznego", które zawiera następujący fragment:

„Uznając znaczenie ram Tarczy Prywatności [Unia Europejska]–USA, w niniejszym memorandum przedstawiono proces wdrażania nowego mechanizmu, zgodnie z [PPD-28], w odniesieniu do rozpoznania radioelektronicznego […].

[…] Prezydent Obama zapowiedział wydanie nowej dyrektywy prezydenckiej, PPD-28, w celu jasnego określenia, co robimy, a czego nie, jeżeli chodzi o obserwację prowadzoną za granicą.

Na podstawie sekcji 4 lit. d) [PPD-28] sekretarz stanu jest zobowiązany wyznaczyć »starszego koordynatora ds. międzynarodowej dyplomacji w dziedzinie technologii informacyjnej« (»starszy koordynator«), który będzie pełnił funkcję »osoby odpowiedzialnej za kontakty z rządami zagranicznymi, które pragną zgłosić swoje obawy dotyczące działań z zakresu rozpoznania radioelektronicznego prowadzonych przez Stany Zjednoczone«.

[…]

1) [Starszy koordynator] będzie pełnił rolę Rzecznika ds. Tarczy Prywatności i […] będzie ściśle współpracował z odpowiednimi urzędnikami z innych departamentów i agencji, którzy są odpowiedzialni za rozpatrywanie wniosków zgodnie z obowiązującymi przepisami i polityką Stanów Zjednoczonych. Rzecznik działa niezależnie od Wspólnoty Wywiadowczej. Rzecznik podlega bezpośrednio sekretarzowi stanu, który zapewni, by wykonywał on zadania w sposób obiektywny i nie ulegał niepożądanym wpływom, które mogłyby wywrzeć skutek na odpowiedź, której należy udzielić.

[…]".

49 W załączniku VI do decyzji w sprawie Tarczy Prywatności zostało zawarte pismo z dnia 21 czerwca 2016 r., które zostało skierowane przez urząd dyrektora krajowych służb wywiadowczych [Office of the Director of National Intelligence] do departamentu handlu USA oraz do urzędu ds. handlu międzynarodowego w departamencie handlu [International Trade Administration], w którym wskazano, że PPD-28 umożliwia „»hurtowe« gromadzenie […] względnie dużego wolumenu informacji lub danych gromadzonych w wyniku rozpoznania radioelektronicznego w sytuacji, gdy Wspólnota Wywiadowcza nie może stosować identyfikatora związanego z namierzaną osobą […], by skupić gromadzenie danych na konkretnych celach".

Postępowanie główne i pytania prejudycjalne

50 Maximillian Schrems, mieszkający w Austrii obywatel tego kraju, jest użytkownikiem sieci społecznościowej Facebook (zwanej dalej „Facebookiem") począwszy od 2008 r.

51 Od wszystkich osób mieszkających na terytorium Unii i chcących używać Facebooka wymagane jest zawarcie, w chwili rejestracji, umowy ze spółką Facebook Ireland, będącą spółką zależną spółki dominującej Facebook Inc., mającej siedzibę w Stanach Zjednoczonych. Dane osobowe użytkowników Facebooka mieszkających na terytorium Unii są, w całości lub częściowo, przekazywane na serwery spółki Facebook Inc., położone na terytorium Stanów Zjednoczonych, gdzie dane te są przetwarzane.

52 W dniu 25 czerwca 2013 r. M. Schrems wniósł do komisarza skargę, w której zwrócił się zasadniczo o zakazanie spółce Facebook Ireland przekazywania jego danych osobowych do Stanów Zjednoczonych; w tej skardze podniósł on, że prawo i praktyka obowiązujące w tym państwie nie zapewniają wystarczającej ochrony danych osobowych zatrzymywanych na jego terytorium przed prowadzonymi w nim przez władze publiczne działaniami nadzorczymi. Skarga ta została oddalona w szczególności ze względu na to, że Komisja w decyzji 2000/520 stwierdziła, iż Stany Zjednoczone zapewniają odpowiedni stopień ochrony.

53 High Court (wysoki trybunał, Irlandia), przed którym M. Schrems zaskarżył oddalenie jego skargi, zwrócił się do Trybunału z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w przedmiocie wykładni i ważności decyzji 2000/520. Wyrokiem z dnia 6 października 2015 r., Schrems (C-362/14, EU:C:2015:650), Trybunał uznał tę decyzję za nieważną.

54 W następstwie tego wyroku sąd odsyłający uchylił oddalenie skargi M. Schremsa i przekazał ją komisarzowi do ponownego rozpoznania. W ramach wszczętego przez komisarza dochodzenia Facebook Ireland wyjaśniła, że znaczna część danych osobowych została przekazana Facebook Inc. na podstawie standardowych klauzul ochrony danych zawartych w załączniku do decyzji w sprawie klauzul standardowych. Mając na uwadze te okoliczności, komisarz wezwał M. Schremsa do przeformułowania skargi.

55 W złożonej w dniu 1 grudnia 2015 r. skardze w zmienionym brzmieniu M. Schrems podniósł w szczególności, że prawo amerykańskie nakłada na Facebook Inc. obowiązek udostępnienia władzom amerykańskim, takim jak National Security Agency (NSA) i Federal Bureau of Investigation (FBI), przekazanych tej spółce danych osobowych. Twierdził on, że ze względu na to, iż dane te były wykorzystywane w ramach różnych programów nadzoru w sposób niezgodny z art. 7, 8 i 47 karty, decyzja w sprawie klauzul standardowych nie może uzasadniać przekazania tych danych do Stanów Zjednoczonych. W tych okolicznościach M. Schrems zwrócił się do komisarza o zakazanie lub zawieszenie przekazywania jego danych osobowych do Facebook Inc.

56 W dniu 24 maja 2016 r. komisarz opublikował „projekt decyzji" przedstawiający pokrótce wstępne wnioski z przeprowadzonego przezeń dochodzenia. W projekcie tym uznał on wstępnie, że istnieje prawdopodobieństwo, iż przekazywane do Stanów Zjednoczonych dane osobowe obywateli Unii mogą być udostępniane organom władz amerykańskich i przetwarzane przez nie w sposób niezgodny z art. 7 i 8 karty oraz że w prawie amerykańskim nie przewidziano dla tych obywateli środków zaskarżenia, które byłyby zgodne z art. 47 karty. Komisarz uznał, że brakowi temu nie mogą zaradzić standardowe klauzule ochrony danych zawarte w załączniku do decyzji w sprawie klauzul standardowych, ponieważ przewidują one w przypadku osób, których dane dotyczą, jedynie mające źródło w umowie uprawnienia, na które mogą się one powołać przeciwko podmiotom przekazującym i odbierającym dane, które to klauzule nie wiążą jednak władz amerykańskich.

57 Będąc zdania, że w tych okolicznościach sformułowana na nowo skarga M. Schremsa dotyczy ważności decyzji w sprawie klauzul standardowych, komisarz w dniu 31 maja 2016 r., opierając się na orzecznictwie wynikającym z wyroku z dnia 6 października 2015 r., Schrems (C-362/14, EU:C:2015:650, pkt 65) zwrócił się do High Court (wysokiego trybunału), aby ten skierował do Trybunału pytanie w tym względzie. Postanowieniem z dnia 4 maja 2018 r. High Court (wysoki trybunał) zwrócił się do Trybunału z niniejszym odesłaniem prejudycjalnym.

58 High Court (wysoki trybunał) załączył do tego wniosku o wydanie orzeczenia w trybie prejudycjalnym wydany w dniu 3 października 2017 r. wyrok, w którym przedstawił wyniki analizy dowodów przedstawionych przed nim w ramach postępowania krajowego, w którym uczestniczył rząd amerykański.

59 W wyroku tym, do którego wniosek o wydanie orzeczenia w trybie prejudycjalnym wielokrotnie odsyła, sąd odsyłający wskazał, że co do zasady ma on nie tylko prawo, ale również obowiązek zbadania wszystkich podniesionych przed nim faktów i argumentów w celu wydania na ich podstawie rozstrzygnięcia, czy zachodzi konieczność wystąpienia z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym. W każdym razie jest on zobowiązany do uwzględnienia ewentualnych zmian przepisów prawa, jakie zaszły w okresie pomiędzy wniesieniem skargi a przeprowadzoną przed nim rozprawą. Sąd ten wyjaśnił, że w ramach postępowania głównego jego ocena nie ogranicza się do zarzutów nieważności podniesionych przez komisarza, wobec czego może on również uwzględnić z urzędu inne zarzuty nieważności i na ich właśnie podstawie wystąpić z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym.

60 Zgodnie z zawartymi w tym wyroku ustaleniami działalność wywiadowcza prowadzona przez władze amerykańskie w odniesieniu do danych osobowych przekazywanych do Stanów Zjednoczonych opiera się w szczególności na art. 702 FISA i na rozporządzeniu wykonawczym nr 12333.

61 W zakresie dotyczącym art. 702 FISA sąd odsyłający wyjaśnia w tym samym wyroku, że przepis ten upoważnia Attorney General (prokuratora generalnego, Stany Zjednoczone) i Director of National Intelligence (DNI) (dyrektora państwowych służb wywiadu, Stany Zjednoczone) działających łącznie i po uzyskaniu zgody FISC, do wydania, w celu pozyskiwania „zagranicznych informacji wywiadowczych", zezwolenia na prowadzenie czynności nadzorczych wobec znajdujących się poza terytorium Stanów Zjednoczonych osób niebędących obywatelami amerykańskimi; przepis ten stanowi w szczególności podstawę prawną dla programów nadzoru PRISM i UPSTREAM. W ramach programu

PRISM dostawcy usług internetowych są, zgodnie z ustaleniami tego sądu, zobowiązani dostarczać NSA wszystkie komunikaty wychodzące z lub przychodzące do „selektora"; część tych komunikatów jest również przekazywana FBI i Central Intelligence Agency (CIA) (centralnej agencji wywiadowczej).

62 Co się tyczy programu UPSTREAM, sąd ten stwierdził, że w ramach tego programu przedsiębiorstwa telekomunikacyjne korzystające z „infrastruktury szkieletowej" internetu – czyli sieci kabli, przełączników sieciowych i routerów – są zobowiązane umożliwić NSA kopiowanie i filtrowanie internetowego ruchu danych w celu pozyskiwania komunikatów wychodzących od, przychodzących do lub dotyczących niebędącej obywatelem amerykańskim osoby skojarzonej z danym „selektorem". Zgodnie z ustaleniami tego samego sądu w ramach wspomnianego programu NSA ma dostęp zarówno do metadanych, jak i treści komunikatów.

63 Jeśli chodzi o rozporządzenie wykonawcze nr 12333, sąd odsyłający stwierdza, że umożliwia ono NSA uzyskanie dostępu do danych, które są „w tranzycie" w kierunku terytorium Stanów Zjednoczonych poprzez dostęp do podwodnych kabli spoczywających na dnie Oceanu Atlantyckiego, a także gromadzenie i zatrzymywanie tych danych, zanim jeszcze dotrą one do Stanów Zjednoczonych i będą tam podlegać przepisom FISA. Sąd ten wyjaśnia, że czynności prowadzone na podstawie rozporządzenia wykonawczego nr 12333 nie zostały uregulowane ustawowo.

64 Jeśli chodzi o ograniczenia działalności rozpoznawczej, sąd odsyłający kładzie nacisk na fakt, że osobom niebędącym obywatelami amerykańskimi przysługują wyłącznie gwarancje przewidziane w PPD-28 i że akt ten ogranicza się do wskazania, że działalność ta powinna być „w jak największym stopniu dostosowana do indywidualnych potrzeb" (*as tailored as feasible*). Na podstawie swoich ustaleń sąd ten uważa, że Stany Zjednoczone przetwarzają dane osobowe na skalę masową i bez rozróżnienia, nie zapewniając ochrony merytorycznie równoważnej tej zagwarantowanej w art. 7 i 8 karty.

65 Co się tyczy ochrony sądowej, sąd ten wskazuje, że obywatele Unii nie mają dostępu do tych samych sądowych środków prawnych, którymi mogą posłużyć się obywatele amerykańscy w obronie przeciwko przetwarzaniu danych osobowych przez władze amerykańskie, ponieważ czwarta poprawka do Constitution of the United States (konstytucji Stanów Zjednoczonych), będąca najważniejszym środkiem ochrony przed prowadzeniem niezgodnego z prawem nadzoru, nie znajduje w przypadku obywateli Unii zastosowania. W tym względzie sąd odsyłający wyjaśnia, że korzystanie ze środków prawnych, które pozostają do ich dyspozycji, wiąże się z istotnymi utrudnieniami, a w szczególności istnieniem obowiązku – spełnienie którego jest jego zdaniem nadmiernie utrudnione – wykazania przysługującej im legitymacji czynnej. Ponadto zgodnie z ustaleniami tego sądu czynności prowadzone przez NSA na podstawie rozporządzenia wykonawczego nr 12333 nie podlegają kontroli sądowej i zaskarżeniu. Wreszcie wspomniany sąd uważa, że ze względu na to, iż jego zdaniem Rzecznik ds. Tarczy Prywatności nie stanowi sądu w rozumieniu art. 47 karty, prawo amerykańskie nie zapewnia obywatelom Unii stopnia ochrony merytorycznie równoważnego temu, który jest gwarantowany ustanowionym w tym artykule prawem podstawowym.

66 We wniosku o wydanie orzeczenia w trybie prejudycjalnym sąd odsyłający wyjaśnia ponadto, że strony postępowania głównego spierają się w szczególności co do kwestii możliwości zastosowania prawa Unii do przekazywania do państwa trzeciego danych osobowych, które mogą być przetwarzane przez organy tego państwa w szczególności do celów bezpieczeństwa narodowego, a także elementów, które należy wziąć pod uwagę do celów oceny tego, czy zapewniany przez to państwo stopień ochrony jest odpowiedni. W szczególności sąd ten zauważa, że zdaniem Facebook Ireland ustalenia Komisji dotyczące odpowiedniego stopnia ochrony zapewnianego przez państwo trzecie, takie jak te zawarte w decyzji w sprawie Tarczy Prywatności, wiążą organy nadzorcze również w kontekście przekazywania danych osobowych w oparciu o standardowe klauzule ochrony danych zawarte w załączniku do decyzji w sprawie klauzul standardowych.

67 W odniesieniu do tych standardowych klauzul ochrony danych sąd ten zastanawia się, czy decyzja w sprawie klauzul standardowych może zostać uznana za ważną, nawet jeśli zdaniem tego sądu wspomniane klauzule nie mają charakteru wiążącego wobec władz państwowych danego państwa trzeciego i w związku z tym nie są w stanie zaradzić ewentualnemu brakowi odpowiedniego stopnia ochrony w tym państwie. W tym względzie sąd odsyłający uważa, że przyznana właściwym organom państw członkowskich w art. 4 ust. 1 lit. a) decyzji 2010/87 w brzmieniu poprzedzającym wejście w życie decyzji wykonawczej 2016/2297 możliwość zakazania przekazywania danych osobowych do państwa trzeciego nakładającego na podmiot przekazujący dane obowiązki niezgodne z gwarancjami zawartymi w tych samych klauzulach wskazuje na to, że stan prawny państwa trzeciego może uzasadniać ten zakaz przekazywania danych, nawet jeśli nastąpiło ono na podstawie standardowych klauzul ochrony danych zawartych w załączniku do decyzji w sprawie klauzul standardowych i, co za tym idzie, świadczy o tym, że klauzule te mogą być niewystarczające do zapewnienia odpowiedniej ochrony. Niemniej jednak sąd odsyłający zastanawia się nad zakresem przysługującego komisarzowi uprawnienia do zakazania przekazywania danych na podstawie tych klauzul, uznając jednocześnie, że uprawnienia dyskrecjonalne nie są wystarczające, aby zapewnić odpowiednią ochronę.

68 W tych okolicznościach High Court (wysoki trybunał) postanowił zawiesić postępowanie i zwrócić się do Trybunału z następującymi pytaniami prejudycjalnymi:

„1) W sytuacji gdy dane osobowe są przekazywane przez prywatne przedsiębiorstwo z państwa członkowskiego [Unii] do prywatnego przedsiębiorstwa w państwie trzecim w celach komercyjnych na podstawie decyzji [w sprawie klauzul standardowych] i mogą być dalej przetwarzane w tym państwie trzecim przez jego organy dla celów bezpieczeństwa narodowego, ale także dla celów egzekwowania prawa i prowadzenia spraw zagranicznych w tym kraju trzecim, czy prawo Unii (w tym także karta) ma zastosowanie do przekazywania danych niezależnie od postanowień art. 4 ust. 2 TUE w odniesieniu do bezpieczeństwa narodowego i od postanowień art. 3 ust. 2 tiret pierwsze dyrektywy [95/46] w odniesieniu do bezpieczeństwa publicznego, obronności i bezpieczeństwa państwa?

2) a) Przy określaniu, czy przekazywanie danych w oparciu o decyzję [w sprawie klauzul standardowych] z [Unii] do państwa trzeciego, gdzie mogą one być dalej przetwarzane dla celów bezpieczeństwa narodowego, czy właściwym punktem odniesienia dla celów dyrektywy [95/46] jest:
   (i) karta, traktat UE, traktat FUE, dyrektywa [95/46], [europejska Konwencja o ochronie praw człowieka i podstawowych wolności, podpisana w Rzymie w dniu 4 listopada 1950 r.] (czy też jakikolwiek inny przepis prawa Unii); czy
   (ii) prawa krajowe jednego lub większej liczby państw członkowskich?
   b) Jeżeli właściwym punktem odniesienia jest ppkt (ii), czy obejmuje on także praktyki w kontekście bezpieczeństwa narodowego w jednym lub większej liczbie państw członkowskich?

3) Przy ocenie, czy państwo trzecie zapewnia stopień ochrony wymagany przez prawo Unii Europejskiej dla danych osobowych przekazywanych do tego państwa dla celów art. 26 dyrektywy [95/46], czy stopień ochrony w państwie trzecim powinien być oceniany poprzez odniesienie do:
   a) obowiązujących przepisów w państwie trzecim, wynikających z jego prawa krajowego lub zobowiązań międzynarodowych oraz z praktyk mających na celu zapewnienie zgodności z tymi przepisami, zasad wykonywania zawodu i środków bezpieczeństwa, które są przestrzegane w tym państwie trzecim;

   czy
   b) przepisów, o których mowa w lit. a) wraz z praktykami administracyjnymi, regulacyjnymi i praktykami w zakresie zgodności oraz polityką w zakresie środków bezpieczeństwa, procedurami, protokołami, mechanizmami kontroli i systemami pozasądowego rozstrzygania sporów istniejącymi w tym państwie trzecim?

4) Przy uwzględnieniu stanu faktycznego ustalonego przez High Court [wysoki trybunał] w odniesieniu do prawa Stanów Zjednoczonych, czy przekazywanie danych osobowych z [Unii] do Stanów Zjednoczonych na podstawie decyzji [w sprawie klauzul standardowych] narusza prawa jednostek wynikające z art. 7 lub 8 karty?

5) Przy uwzględnieniu stanu faktycznego ustalonego przez High Court [wysoki trybunał] w odniesieniu do prawa Stanów Zjednoczonych, jeżeli dane osobowe są przekazywane z [Unii] do Stanów Zjednoczonych na podstawie decyzji [w sprawie klauzul standardowych]]:
   a) Czy stopień ochrony w prawie Stanów Zjednoczonych zapewnia poszanowanie istoty prawa jednostek do korzystania ze środków prawnych w związku z naruszeniem ich praw do prywatności danych osobowych zagwarantowanych przez art. 47 karty?

   Jeżeli odpowiedź na pytanie piąte a) jest twierdząca:
   b) Czy ograniczenia, jakie nakłada prawo Stanów Zjednoczonych na prawo jednostki do korzystania z sądowych środków ochrony prawnej w kontekście bezpieczeństwa narodowego Stanów Zjednoczonych, są proporcjonalne w rozumieniu art. 52 karty i nie wykraczają poza to, co jest niezbędne w społeczeństwie demokratycznym dla celów bezpieczeństwa narodowego?

6) a) Jaki jest stopień ochrony, który należy zapewnić przy przekazywaniu danych osobowych do państwa trzeciego na podstawie standardowych klauzul umownych przyjętych zgodnie z decyzją Komisji w oparciu o art. 26 ust. 4 w świetle przepisów dyrektywy [95/46], a w szczególności art. 25 i 26 w związku z kartą?
   b) Jakie kwestie należy wziąć pod uwagę przy ocenie, czy stopień ochrony danych osobowych przekazywanych do państwa trzeciego na podstawie decyzji [w sprawie klauzul standardowych] spełnia wymogi dyrektywy [95/46] i karty?

7) Czy okoliczność, że standardowe klauzule ochrony obowiązują pomiędzy podmiotem przekazującym a odbierającym dane i nie są wiążące dla władz krajowych państwa trzeciego, które mogą wymagać od podmiotu odbierającego dane udostępniania jego służbom bezpieczeństwa w celu dalszego przetwarzania danych osobowych przekazywanych na mocy klauzul przewidzianych w decyzji [w sprawie klauzul standardowych], wyklucza zapewnienie przez te klauzule odpowiednich zabezpieczeń zgodnie z art. 26 ust. 2 dyrektywy [95/46]?

8) Jeżeli podmiot odbierający dane w państwie trzecim jest objęty przepisami dotyczącymi nadzoru, które zdaniem organu ochrony danych są sprzeczne ze [standardowymi klauzulami ochrony] lub art. 25 i 26 dyrektywy [95/46] lub kartą, czy organ ds. ochrony danych jest zobowiązany do skorzystania ze swoich uprawnień wykonawczych zgodnie z art. 28 ust. 3 dyrektywy [95/46] w celu zawieszenia przepływu danych, czy też wykonywanie tych uprawnień jest ograniczone do sytuacji wyjątkowych, w świetle [motywu 11 decyzji w sprawie klauzul standardowych], względnie czy organ ochrony danych w ramach przysługującego mu uznania może nie zawieszać przepływu danych?

9) a) Dla celów art. 25 ust. 6 dyrektywy [95/46], czy decyzja [w sprawie Tarczy Prywatności] stanowi ustalenie o powszechnym zastosowaniu wiążące dla organów ochrony danych oraz sądów państw członkowskich, stwierdzające, że Stany Zjednoczone zapewniają odpowiedni stopień ochrony w rozumieniu art. 25 ust. 2 dyrektywy [95/46], co wynika z prawa krajowego Stanów Zjednoczonych lub z międzynarodowych zobowiązań, jakie państwo to przyjęło?
   b) Jeżeli nie, jakie znaczenie, jeśli w ogóle, ma decyzja [w sprawie Tarczy Prywatności] przy prowadzeniu oceny adekwatności zabezpieczeń przewidzianych dla danych przekazywanych do Stanów Zjednoczonych na mocy decyzji [w sprawie klauzul standardowych]?

10) Przy uwzględnieniu ustaleń High Court [wysokiego trybunału] w odniesieniu do prawa Stanów Zjednoczonych, czy powołanie Rzecznika ds. Tarczy Prywatności zgodnie z załącznikiem A do załącznika III do decyzji [w sprawie Tarczy Prywatności] w związku z istniejącym systemem w Stanach Zjednoczonych zapewnia, że prawo Stanów Zjednoczonych przewiduje środek ochrony prawnej dla osób, których dane osobowe są przekazywane do Stanów Zjednoczonych na podstawie decyzji [w sprawie klauzul standardowych], zgodny z art. 47 karty?

11) Czy decyzja [w sprawie klauzul standardowych] narusza art. 7, 8 lub 47 karty?".

W przedmiocie dopuszczalności wniosku o wydanie orzeczenia w trybie prejudycjalnym

69 Facebook Ireland oraz rządy niemiecki i Zjednoczonego Królestwa podnoszą, że niniejszy wniosek o wydanie orzeczenia w trybie prejudycjalnym jest niedopuszczalny.

70 W ramach podniesionego przez Facebook Ireland zarzutu niedopuszczalności spółka ta zauważa, że przepisy dyrektywy 95/46, na których opierają się pytania prejudycjalne, zostały uchylone przez RODO.

71 W tym względzie, choć prawdą jest, że dyrektywa 95/46 została uchylona na mocy art. 94 ust. 1 RODO ze skutkiem od dnia 25 maja 2018 r., to jednak dyrektywa ta obowiązywała jeszcze w chwili złożenia w dniu 4 maja 2018 r. niniejszego wniosku o wydanie orzeczenia w trybie prejudycjalnym, który wpłynął do Trybunału w dniu 9 maja 2018 r. Ponadto art. 3 ust. 2 tiret pierwsze, art. 25 i 26 oraz art. 28 ust. 3 dyrektywy 95/46, do których odnoszą się pytania prejudycjalne, zostały zasadniczo powtórzone, odpowiednio, w art. 2 ust. 2 oraz w art. 45, 46 i 58 RODO. Poza tym należy przypomnieć, że zadaniem Trybunału jest dokonanie wykładni wszystkich przepisów prawa Unii, jakie są niezbędne sądom krajowym do rozstrzygnięcia zawisłych przed nimi sporów, nawet jeżeli przepisy te nie są wyraźnie wskazane w pytaniach zadanych Trybunałowi (wyrok z dnia 2 kwietnia 2020 r., Ruska Federacija, C-897/19 PPU, EU:C:2020:262, pkt 43 i przytoczone tam orzecznictwo). Z tych różnych względów okoliczność polegająca na tym, że sąd odsyłający zadał pytania prejudycjalne, powołując się wyłącznie na przepisy dyrektywy 95/46, nie może pociągać za sobą niedopuszczalności niniejszego wniosku o wydanie orzeczenia w trybie prejudycjalnym.

72 Rząd niemiecki opiera natomiast swój zarzut niedopuszczalności na okoliczności polegającej, po pierwsze, na tym, że komisarz wyraził jedynie wątpliwości, a nie ostateczną opinię, co do kwestii ważności decyzji w sprawie klauzul standardowych, zaś, po drugie, sąd odsyłający nie sprawdził tego, czy M. Schrems nie wyraził jednoznacznie zgody na przekazanie rozpatrywanych w postępowaniu głównym danych, co, gdyby okazało się prawdą, skutkowałoby tym, że udzielenie odpowiedzi na to pytanie okazałoby się zbędne. Wreszcie zdaniem rządu Zjednoczonego Królestwa pytania prejudycjalne mają charakter hipotetyczny, ponieważ sąd ten nie stwierdził, że rzeczywiście doszło do przekazania danych na podstawie wspomnianej decyzji.

73 Zgodnie z utrwalonym orzecznictwem Trybunału jedynie do sądu krajowego, przed którym zawisł spór i na którym spoczywa odpowiedzialność za mające zapaść rozstrzygnięcie, należy ustalenie, czy, w celu wydania rozstrzygnięcia i przy uwzględnieniu specyfiki danej sprawy, zachodzi potrzeba uzyskania orzeczenia w trybie prejudycjalnym, jak i zasadności zadawanych Trybunałowi pytań. W konsekwencji, jeśli postawione pytania dotyczą wykładni lub ważności prawa Unii, Trybunał jest co do zasady zobowiązany do wydania orzeczenia. Wynika stąd, że pytania zadane przez sądy krajowe korzystają z domniemania posiadania znaczenia dla sprawy. Odmowa wydania przez Trybunał orzeczenia w trybie prejudycjalnym, o które wnioskował sąd krajowy, jest możliwa tylko wtedy, gdy okazuje się, że wykładnia, o którą się zwrócono, nie ma żadnego związku ze stanem faktycznym lub przedmiotem sporu w postępowaniu głównym, gdy problem jest natury hipotetycznej bądź gdy Trybunał nie dysponuje informacjami w zakresie stanu faktycznego lub prawnego niezbędnymi do udzielenia

użytecznej odpowiedzi na pytania (wyroki: z dnia 16 czerwca 2015 r., Gauweiler i in., C-62/14,, EU:C:2015:400, pkt 24, 25; z dnia 2 października 2018 r., Ministerio Fiscal, C-207/16, EU:C:2018:788, pkt 45; a także z dnia 19 grudnia 2019 r., Dobersberger, C-16/18, EU:C:2019:1110, pkt 18, 19).

74 W niniejszym przypadku wniosek o wydanie orzeczenia w trybie prejudycjalnym zawiera w zakresie stanu faktycznego i prawnego informacje, które są wystarczające dla zrozumienia zakresu zadanych pytań. Ponadto, co najważniejsze, żaden pozostający do dyspozycji Trybunału element akt sprawy nie pozwala uznać, że żądana wykładnia prawa Unii nie ma związku ze stanem faktycznym lub przedmiotem sporu w postępowaniu głównym lub ma charakter hipotetyczny, w szczególności z uwagi na to, że rozpatrywane w postępowaniu głównym dane osobowe są przekazywane w oparciu o wyraźną zgodę osoby, której dane dotyczą, nie zaś decyzję w sprawie klauzul standardowych. Zgodnie bowiem z informacjami zawartymi w tym wniosku Facebook Ireland przyznała, że przekazuje Facebook Inc. dane osobowe swoich abonentów zamieszkałych w Unii i że znaczna część tego przekazywania, którego zgodność z prawem jest kwestionowana przez M. Schremsa, jest dokonywana na podstawie standardowych klauzul ochrony danych zawartych w załączniku do decyzji w sprawie klauzul standardowych.

75 Ponadto dla dopuszczalności niniejszego wniosku o wydanie orzeczenia w trybie prejudycjalnym bez znaczenia jest to, że komisarz nie wyraził ostatecznej opinii na temat ważności tej decyzji, ponieważ sąd odsyłający uważa, że odpowiedź na pytania prejudycjalne dotyczące wykładni i ważności przepisów prawa Unii jest niezbędna do rozstrzygnięcia sporu w postępowaniu głównym.

76 Z powyższego wynika, że wniosek o wydanie orzeczenia w trybie prejudycjalnym jest dopuszczalny.

W przedmiocie pytań prejudycjalnych

77 Na wstępie należy przypomnieć, że postępowanie w sprawie niniejszego wniosku o wydanie orzeczenia w trybie prejudycjalnym zostało zapoczątkowane wniesioną przez M. Schremsa do komisarza skargą mającą na celu nakazanie przezeń zawieszenia lub zakazania na przyszłość przekazywania przez Facebook Ireland jego danych osobowych spółce Facebook Inc. Choć zaś te pytania prejudycjalne odnoszą się do przepisów dyrektywy 95/46, bezsporne jest, że komisarz nie wydał jeszcze ostatecznej decyzji w sprawie tej skargi, jako że dyrektywa ta została uchylona i zastąpiona przez RODO ze skutkiem od dnia 25 maja 2018 r.

78 Ten brak decyzji krajowej odróżnia sytuację rozpatrywaną w postępowaniu głównym od tych, w których wydano wyroki z dnia 24 września 2019 r., Google (zakres terytorialny usunięcia linków) (C-507/17, EU:C:2019:772) i z dnia 1 października 2019 r., Planet49 (C-673/17, EU:C:2019:801), które dotyczyły decyzji wydanych przed uchyleniem tej dyrektywy.

79 Tak więc na pytania prejudycjalne należy odpowiadać w świetle przepisów RODO, nie zaś tych zawartych w dyrektywie 95/46.

W przedmiocie pytania pierwszego

80 Poprzez pytanie pierwsze sąd odsyłający dąży zasadniczo do ustalenia, czy art. 2 ust. 1 i art. 2 ust. 2 lit. a), b) i d) RODO w związku z art. 4 ust. 2 TUE należy interpretować w ten sposób, że zakres zastosowania tego rozporządzenia obejmuje przekazywanie przez podmiot gospodarczy z siedzibą w państwie członkowskim danych osobowych innemu podmiotowi gospodarczemu z siedzibą w państwie trzecim, jeżeli w trakcie tego przekazywania lub w jego następstwie dane te mogą być przetwarzane przez organy władz tego państwa trzeciego do celów związanych z bezpieczeństwem publicznym, obroną i bezpieczeństwem państwa.

81 W tym względzie należy na wstępie zauważyć, że przepis zawarty w art. 4 ust. 2 TUE, zgodnie z którym bezpieczeństwo narodowe państw członkowskich pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego, dotyczy wyłącznie państw członkowskich Unii. W konsekwencji przepis ten pozostaje w niniejszym przypadku bez znaczenia dla celów wykładni art. 2 ust. 1 i art. 2 ust. 2 lit. a), b) i d) RODO.

82 Zgodnie z brzmieniem art. 2 ust. 1 RODO ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. Zgodnie z art. 4 pkt 2 tego rozporządzenia „przetwarzanie" oznacza „operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany"; jako przykłady takiego przetwarzania wskazane zostały „ujawnianie poprzez przesłanie [i] rozpowszechnianie lub innego rodzaju udostępnianie", bez wprowadzania rozróżnienia w zależności od tego, czy te operacje są przeprowadzane w obrębie Unii czy też mają jakiś związek z państwami trzecimi. Ponadto zgodnie z tym rozporządzeniem przekazywanie danych osobowych do państw trzecich odbywa się na szczególnych zasadach określonych w jego rozdziale V, zatytułowanym „Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych"; rozporządzenie to przyznaje ponadto organom nadzorczym określone w jego art. 58 ust. 2 lit. j) szczególne uprawnienia w tym względzie.

83 Wynika z tego, że operacja polegająca na przekazywaniu danych osobowych z państwa członkowskiego do państwa trzeciego stanowi jako taka przetwarzanie danych osobowych w rozumieniu art. 4 pkt 2 RODO, dokonywane na terytorium państwa członkowskiego, do którego to przetwarzania rozporządzenie ma zastosowanie na podstawie jego art. 2 ust. 1 [zob. analogicznie, w odniesieniu do art. 2 lit. b) i art. 3 ust. 1 dyrektywy 95/46, wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 45 i przytoczone tam orzecznictwo].

84 Co się tyczy kwestii tego, czy taką operację można uznać za wyłączoną z zakresu zastosowania RODO na podstawie jego art. 2 ust. 2, należy przypomnieć, że przepis ten przewiduje wyjątki dotyczące określonego w art. 2 ust. 1 tego rozporządzenia jego zakresu zastosowania oraz że wyjątki te powinny być interpretowane w sposób ścisły (zob. analogicznie, w odniesieniu do art. 3 ust. 2 dyrektywy 95/46, wyrok z dnia 10 lipca 2018 r., Jehovan todistajat, C-25/17, EU:C:2018:551, pkt 37 i przytoczone tam orzecznictwo).

85 W niniejszej sprawie, ze względu na to, że do rozpatrywanego w postępowaniu głównym przekazywania dochodzi między Facebook Ireland a Facebook Inc., czyli pomiędzy dwiema osobami prawnymi, przekazywanie to nie wchodzi w zakres zastosowania art. 2 ust. 2 lit. c) RODO, który dotyczy przetwarzania danych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze. Przekazywanie to nie stanowi też jednego z wyjątków określonych w art. 2 ust. 2 lit. a), b) i d) tego rozporządzenia, ponieważ rodzaje czynności, które zostały w nim wymienione tytułem przykładu, stanowią w każdym wypadku działalność właściwą państwom i władzom państwowym, odmienną od dziedzin działalności jednostek (zob. analogicznie, w odniesieniu do art. 3 ust. 2 dyrektywy 95/46, wyrok z dnia 10 lipca 2018 r., Jehovan todistajat, C-25/17, EU:C:2018:551, pkt 38 i przytoczone tam orzecznictwo).

86 Tymczasem możliwość polegająca na tym, że dane osobowe przekazywane między dwoma podmiotami gospodarczymi w celach handlowych będą, w trakcie lub w następstwie tego przekazywania, podlegać przetwarzaniu przez organy władz danego państwa trzeciego do celów związanych z bezpieczeństwem publicznym, obronnością i bezpieczeństwem państwa, nie może wyłączać tego przekazywania z zakresu stosowania RODO.

87 Ponadto, ustanawiając spoczywający na Komisji przy dokonywaniu oceny odpowiedniego stopnia ochrony zapewnianej przez państwo trzecie wyraźny obowiązek uwzględnienia w szczególności „odpowiednie[go] ustawodawstw[a] – zarówno ogólne[go], jak i sektorowe[go] – w tym w dziedzinie

bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego oraz dostępu organów publicznych do danych osobowych, a także wdrażanie takiego ustawodawstwa", samo brzmienie art. 45 ust. 2 lit. a) tego rozporządzenia świadczy o tym, że ewentualne przetwarzanie przez kraj trzeci tego rodzaju danych do celów związanych z bezpieczeństwem publicznym, obronnością i bezpieczeństwem państwa nie wyklucza możliwości zastosowania tego rozporządzenia do przekazywania rozpatrywanego w niniejszej sprawie.

88 Wynika z tego, że takie przekazywanie nie może być wyłączone z zakresu stosowania RODO z tego powodu, że rozpatrywane dane mogą być przetwarzane – w trakcie lub w następstwie tego przekazania – przez organy władzy danego państwa trzeciego dla celów związanych z bezpieczeństwem publicznym, obronnością i bezpieczeństwem państwa.

89 W konsekwencji na pytanie pierwsze należy odpowiedzieć, że art. 2 ust. 1 i 2 RODO należy interpretować w ten sposób, iż zakresem stosowania tego rozporządzenia jest objęte przekazywanie danych osobowych przez podmiot gospodarczy mający siedzibę w jednym państwie członkowskim innemu podmiotowi gospodarczemu z siedzibą w państwie trzecim niezależnie od faktu, że w trakcie tego przekazywania lub w jego następstwie dane te mogą być przetwarzane przez organy władzy danego państwa trzeciego w celach związanych z bezpieczeństwem publicznym, obronnością i bezpieczeństwem państwa.

W przedmiocie pytań drugiego, trzeciego i szóstego

90 W pytaniach drugim, trzecim i szóstym sąd odsyłający zwraca się do Trybunału zasadniczo z pytaniem dotyczącym stopnia ochrony wymaganego przez art. 46 ust. 1 i art. 46 ust. 2 lit. c) RODO w ramach przekazywania danych osobowych do państwa trzeciego na podstawie standardowych klauzul ochrony danych. W szczególności sąd ten zwraca się do Trybunału o wyjaśnienie, jakie czynniki należy wziąć pod uwagę w celu ustalenia, czy ten stopień ochrony pozostaje zapewniony w kontekście takiego przekazywania.

91 Co się tyczy wymaganego stopnia ochrony, z łącznej lektury tych przepisów wynika, że w braku wydawanej na podstawie art. 45 ust. 3 tego rozporządzenia decyzji stwierdzającej odpowiedni stopień ochrony administrator danych lub podmiot przetwarzający mogą przekazywać dane osobowe do państwa trzeciego jedynie wówczas, gdy państwo to przewidziało „odpowiednie zabezpieczenia" i pod warunkiem, że „obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej", przy czym takie odpowiednie zabezpieczenia mogą zostać udzielone w szczególności w drodze przyjmowanych przez Komisję standardowych klauzul ochrony danych.

92 Choć w art. 46 RODO nie wyjaśniono charakteru, jaki mają wymogi wynikające z tego powołania się na „odpowiednie zabezpieczenia", „egzekwowalne prawa" i „skuteczne środki ochrony prawnej", niemniej jednak należy zauważyć, że przepis ten znajduje się w rozdziale V tego rozporządzenia i, co za tym idzie, należy go interpretować w świetle art. 44 wspomnianego rozporządzenia, który jest zatytułowany „Ogólna zasada przekazywania" i stanowi, że „[w]szystkie przepisy [tego] rozdziału należy stosować z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w [tym] rozporządzeniu". Ten stopień ochrony powinien więc być zapewniony niezależnie od podstawy, na jakiej dokonywane jest przekazywanie danych osobowych do państwa trzeciego.

93 Jak bowiem zauważył Rzecznik generalny w pkt 117 opinii, przepisy rozdziału V RODO mają na celu zapewnienie ciągłości stopnia tej ochrony w sytuacji, gdy dane te są przekazywane do państwa trzeciego, zgodnie z celem określonym w motywie 6 tego rozporządzenia.

94 Artykuł 45 ust. 1 zdanie pierwsze RODO przewiduje, że przekazanie danych osobowych do państwa trzeciego jest dozwolone w oparciu o wydaną przez Komisję decyzję, zgodnie z którą to państwo trzecie, terytorium lub określony sektor czy też określone sektory w tym państwie trzecim zapewniają

odpowiedni stopień ochrony. W tym względzie, nie wymagając bynajmniej, aby dane państwo trzecie zapewniało stopień ochrony identyczny jak ten zagwarantowany w unijnym porządku prawnym, wyrażenie „odpowiedni stopień ochrony" należy rozumieć – jak potwierdza to motyw 104 tego rozporządzenia – jako ustanawiające wobec tego państwa trzeciego wymóg rzeczywistego zapewnienia, ze względu na jego ustawodawstwo wewnętrzne lub też zobowiązania międzynarodowe, stopnia ochrony podstawowych praw i wolności merytorycznie równoważnego temu gwarantowanemu w Unii na mocy tego rozporządzenia interpretowanego w związku z kartą. W braku takiego wymogu cel wymieniony w poprzedzającym punkcie zostałby bowiem podważony (zob. analogicznie, w odniesieniu do art. 25 ust. 6 dyrektywy 95/46, wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 73).

95 W tym kontekście motyw 107 RODO stanowi, że w przypadku gdy „państwo trzecie, terytorium lub określony sektor w państwie trzecim […] przestały zapewniać odpowiedni stopień ochrony danych […], przekazywanie danych osobowych do tego państwa trzeciego powinno być zakazane, chyba że spełnione są wymogi [tego rozporządzenia] dotyczące przekazywania danych stanowiących przedmiot odpowiednich zabezpieczeń". W tym względzie w motywie 108 wspomnianego rozporządzenia wyjaśniono, że w braku decyzji stwierdzającej odpowiedni stopień ochrony odpowiednie zabezpieczenia, które powinien zapewnić administrator danych lub podmiot przetwarzający zgodnie z art. 46 ust. 1 tego rozporządzenia, powinny „rekompens[ować] brak ochrony danych w państwie trzecim" w celu „zapewni[enia], by przestrzegane były wymogi ochrony danych oraz prawa osób, których dane dotyczą, takie same jak w przypadku przetwarzania wewnątrzunijnego".

96 Wynika z tego, jak zauważył Rzecznik generalny w pkt 115 opinii, że te odpowiednie zabezpieczenia powinny gwarantować, by prawa przysługujące osobom, których dane są przekazywane na podstawie standardowych klauzul ochrony danych, korzystały, podobnie jak w przypadku przekazywania na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, ze stopnia ochrony merytorycznie równoważnego temu gwarantowanemu w Unii.

97 Sąd odsyłający zastanawia się również nad kwestią, czy ten stopień ochrony merytorycznie równoważny temu gwarantowanemu w Unii należy ustalać w świetle prawa Unii, a w szczególności praw gwarantowanych przez kartę, lub w świetle praw podstawowych chronionych przez europejską Konwencję o ochronie praw człowieka i podstawowych wolności (zwaną dalej „EKPC") lub też w świetle prawa krajowego państw członkowskich.

98 W tym względzie należy przypomnieć, że jakkolwiek zgodnie z art. 6 ust. 3 TUE prawa podstawowe zagwarantowane w EKPC stanowią część prawa Unii jako jego zasady ogólne i jakkolwiek art. 52 ust. 3 karty stanowi, że prawa zawarte w karcie odpowiadające prawom zagwarantowanym w EKPC mają takie samo znaczenie i taki sam zakres jak prawa przyznane przez tę konwencję, to jednak konwencja ta, do czasu przystąpienia do niej Unii, nie stanowi aktu prawnego formalnie obowiązującego w porządku prawnym Unii (wyroki: z dnia 26 lutego 2013 r., Åkerberg Fransson, C-617/10, EU:C:2013:105, pkt 44 i przytoczone tam orzecznictwo; a także z dnia 20 marca 2018 r., Menci, C-524/15, EU:C:2018:197, pkt 22).

99 W tych okolicznościach Trybunał orzekł, że wykładni prawa Unii oraz badania ważności aktów Unii należy dokonywać w świetle praw podstawowych zagwarantowanych w karcie (zob. analogicznie wyrok z dnia 20 marca 2018 r., Menci, C-524/15, EU:C:2018:197, pkt 24).

100 Ponadto z utrwalonego orzecznictwa wynika, że ważności przepisów prawa Unii i, w braku wyraźnego odesłania do prawa krajowego państw członkowskich, ich wykładni nie można oceniać w świetle tego prawa krajowego, nawet rangi konstytucyjnej, w szczególności praw podstawowych w postaci sformułowanej w ich konstytucji krajowej (zob. podobnie wyroki: z dnia 17 grudnia 1970 r., Internationale Handelsgesellschaft, 11/70, EU:C:1970:114, pkt 3; z dnia 13 grudnia 1979 r., Hauer, 44/79, EU:C:1979:290, pkt 14; a także z dnia 18 października 2016 r., Nikiforidis, C-135/15, EU:C:2016:774, pkt 28 i przytoczone tam orzecznictwo).

101 Z powyższego wynika, że skoro z jednej strony przekazywanie danych osobowych takie jak to rozpatrywane w postępowaniu głównym, dokonywane w celach handlowych przez podmiot gospodarczy mający siedzibę w jednym państwie członkowskim, na rzecz innego podmiotu gospodarczego mającego siedzibę w państwie trzecim, jest objęte – jak wynika z odpowiedzi na pytanie pierwsze – zakresem zastosowania RODO, a z drugiej strony rozporządzenie to w szczególności zmierza do, jak wynika z jego motywu 10, zapewnienia spójnego i wysokiego stopnia ochrony osób fizycznych i, w tym celu, zapewnienia spójnego i jednolitego w całej Unii stosowania przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych, stopień ochrony praw podstawowych wymagany w art. 46 ust. 1 tego rozporządzenia należy ustalać na podstawie przepisów tego samego rozporządzenia interpretowanych w świetle zagwarantowanych w karcie praw podstawowych.

102 Sąd odsyłający dąży ponadto do ustalenia, jakie czynniki należy wziąć pod uwagę w celu ustalenia odpowiedniego stopnia ochrony w kontekście przekazywania danych osobowych do państwa trzeciego na podstawie standardowych klauzul ochrony danych przyjętych w zastosowaniu art. 46 ust. 2 lit. c) RODO.

103 W tym względzie, choć przepis ten nie wymienia poszczególnych czynników, które należy wziąć pod uwagę w celu dokonania oceny tego, czy stopień ochrony, jakiego należy przestrzegać w ramach takiego przekazania, jest odpowiedni, o tyle w art. 46 ust. 1 tego rozporządzenia wyjaśniono, że osoby, których dane dotyczą, powinny korzystać z odpowiednich zabezpieczeń oraz winny im przysługiwać egzekwowalne prawa oraz skuteczne środki ochrony prawnej.

104 W tym celu ocena stopnia ochrony, jaką należy przeprowadzić w kontekście takiego przekazania, powinna w szczególności uwzględniać zarówno postanowienia umowne uzgodnione między mającymi siedzibę w Unii administratorem danych lub podmiotem przetwarzającym a odbierającym dane podmiotem mającym siedzibę w danym państwie trzecim, jak i, w odniesieniu do ewentualnego dostępu organów władzy publicznej tego państwa trzeciego do przekazanych w ten sposób danych osobowych, istotne elementy składające się na jego system prawny. W tym względzie elementy, jakie należy wziąć pod uwagę w kontekście art. 46 tego rozporządzenia, odpowiadają tym przedstawionym w niewyczerpujący sposób w jego art. 45 ust. 2.

105 W związku z tym na pytania drugie, trzecie i szóste należy odpowiedzieć, że art. 46 ust. 1 i art. 46 ust. 2 lit. c) RODO należy interpretować w ten sposób, że wymagane przez te przepisy odpowiednie zabezpieczenia, egzekwowalne prawa oraz skuteczne środki ochrony prawnej powinny zapewniać, by prawa osób, których dane osobowe są przekazywane do państwa trzeciego na podstawie klauzul ochrony danych, były chronione w stopniu merytorycznie równoważnym temu gwarantowanemu w Unii przez to rozporządzenie, interpretowane w świetle karty. W tym celu w ramach oceny stopnia ochrony zapewnianego w kontekście takiego przekazywania należy w szczególności uwzględniać zarówno postanowienia umowne uzgodnione między mającymi siedzibę w Unii administratorem danych lub podmiotem przetwarzającym a podmiotem odbierającym dane mającym siedzibę w danym państwie trzecim, jak i, w odniesieniu do ewentualnego dostępu organów władzy publicznej tego państwa trzeciego do przekazywanych w ten sposób danych osobowych, istotne elementy składające się na jego system prawny, w szczególności te wymienione w art. 45 ust. 2 wspomnianego rozporządzenia.

W przedmiocie pytania ósmego

106 Poprzez pytanie ósme sąd odsyłający dąży zasadniczo do ustalenia, czy art. 58 ust. 2 lit. f) i j) RODO należy interpretować w ten sposób, że właściwy organ nadzorczy jest zobowiązany do zawieszenia lub zakazania przekazywania danych osobowych do państwa trzeciego na podstawie standardowych klauzul ochrony danych przyjętych przez Komisję, jeśli ten organ nadzorczy uzna, że klauzule te nie są

lub nie mogą być przestrzegane w tym państwie trzecim, a ochrona przekazywanych danych, jakiej wymaga prawo Unii, a w szczególności art. 45 i 46 RODO oraz karta, nie może być zapewniona, czy też w ten sposób, że korzystanie z tego uprawnienia jest ograniczone do wyjątkowych przypadków.

107 Zgodnie z art. 8 ust. 3 karty oraz z art. 51 ust. 1 i art. 57 ust. 1 lit. a) RODO krajowe organy nadzorcze są odpowiedzialne za kontrolę przestrzegania przepisów Unii dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych. W związku z tym każdy z nich jest uprawniony do sprawdzenia, czy przekazywanie danych osobowych z jego państwa członkowskiego do państwa trzeciego spełnia wymogi ustanowione w tym rozporządzeniu (zob. analogicznie odnośnie do art. 28 dyrektywy 95/46 wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 47).

108 Z przepisów tych wynika, że najważniejszym z zadań wykonywanych przez te organy nadzorcze jest monitorowanie i egzekwowanie stosowania RODO. Wykonywanie tego zadania nabiera szczególnego znaczenia w kontekście przekazywania danych osobowych do państwa trzeciego, ponieważ, jak wynika z samego brzmienia motywu 116 tego rozporządzenia, „[t]ransgraniczne przekazywanie danych osobowych poza Unią może spowodować wzrost ryzyka, że osoby fizyczne nie będą mogły wykonywać prawa do ochrony danych osobowych, w szczególności w celu ochrony przed niezgodnym z prawem wykorzystaniem lub ujawnieniem tych informacji". Na taką okoliczność w motywie tym wyjaśniono, iż „organy nadzorcze mogą uznać, że nie są w stanie rozpatrzyć skargi lub przeprowadzić postępowania w sprawie działalności, która ma miejsce poza granicami ich państwa".

109 Ponadto zgodnie z art. 57 ust. 1 lit. f) RODO każdy organ nadzorczy jest zobowiązany na swoim terytorium rozpatrzyć skargi, które mogą zostać skierowane zgodnie z art. 77 ust. 1 tego rozporządzenia przez każdą osobę, której dane dotyczą, jeżeli ta sądzi, że przetwarzanie tych danych narusza to rozporządzenie, i przeanalizować w koniecznym zakresie ich przedmiot. Organ nadzorczy jest zobowiązany do rozpatrzenia tej skargi z wszelką wymaganą starannością (zob. analogicznie w odniesieniu do art. 25 ust. 6 dyrektywy 95/46; wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 63).

110 W art. 78 ust. 1 i 2 RODO zostało ustanowione przysługujące każdej osobie prawo do skutecznego środka ochrony prawnej przed sądem, w szczególności w sytuacji, gdy organ nadzorczy nie rozpatruje jej skargi. Motyw 141 tego rozporządzenia odwołuje się również do tego „praw[a] do skutecznego środka ochrony prawnej przed sądem, zgodnie z art. 47 karty", w przypadku gdy ten organ nadzorczy „nie podejmuje działania, choć jest to niezbędne do ochrony praw [danej] osoby".

111 Do celów rozpatrywania wniesionych skarg w art. 58 ust. 1 RODO każdemu organowi nadzorczemu zostały przyznane daleko idące uprawnienia w zakresie prowadzonych w tym zakresie postępowań. Jeżeli organ taki po zakończeniu dochodzenia uzna, że osoba, której dane zostały przekazane do państwa trzeciego, nie korzysta w tym państwie z odpowiedniego stopnia ochrony, jest w zastosowaniu prawa Unii zobowiązany zareagować w sposób odpowiedni, aby zaradzić stwierdzonemu brakowi ochrony, i to niezależnie od przyczyn zaistnienia czy też charakteru tego braku. W tym względzie w art. 58 ust. 2 tego rozporządzenia zostały wymienione różnego rodzaju działania naprawcze, które mogą zostać podjęte przez organ nadzorczy.

112 Mimo że dokonanie wyboru odpowiedniego i skutecznego środka należy do organu nadzorczego, a organ ten powinien go dokonać, uwzględniając wszystkie okoliczności towarzyszące rozpatrywanemu przekazywaniu danych osobowych, jest on niemniej jednak zobowiązany wywiązać się z należytą starannością z powierzonego mu zadania polegającego na egzekwowaniu pełnego stosowania RODO.

113 W tym względzie, jak zauważył również Rzecznik generalny w pkt 148 opinii, wspomniany organ jest na podstawie art. 58 ust. 2 lit. f) i j) tego rozporządzenia zobowiązany do zawieszenia lub zakazania przekazywania danych osobowych do państwa trzeciego, jeżeli w świetle wszystkich okoliczności towarzyszących temu przekazywaniu stwierdzi, że standardowe klauzule ochrony danych nie są lub nie mogą być przestrzegane w tym państwie trzecim i że nie można zapewnić wymaganej przez unijne

prawo ochrony przekazywanych danych przy pomocy innych środków, jeśli to przekazywanie nie zostało zawieszone lub zakończone przez samego administratora danych lub jego podmiot przetwarzający z siedzibą w Unii.

114 Wykładni przedstawionej w poprzednim punkcie nie można podważyć za pomocą przedstawionej przez komisarza argumentacji, zgodnie z którą art. 4 decyzji 2010/87 w brzmieniu sprzed wejścia w życie decyzji wykonawczej 2016/2297 w związku z motywem 11 tej decyzji ograniczał tylko do pewnych wyjątkowych sytuacji możliwość skorzystania przez organy nadzorcze z przysługującego im uprawnienia do zawieszenia lub zakazania przekazywania danych osobowych do państwa trzeciego. W wersji wynikającej z decyzji wykonawczej 2016/2297 w art. 4 decyzji w sprawie klauzul standardowych jest bowiem mowa o uprawnieniu, jakie przysługuje tym organom – obecnie na podstawie art. 58 ust. 2 lit. f) i j) RODO – do zawieszenia lub zakazania takiego przekazywania, nie ograniczając w żaden sposób wykonywania tego uprawnienia do przypadków zaistnienia wyjątkowych okoliczności.

115 W każdym razie uprawnienia wykonawcze, które art. 46 ust. 2 lit. c) RODO przyznaje Komisji celem przyjęcia standardowych klauzul ochrony danych, nie przyznają jej kompetencji do ograniczania uprawnień przysługujących organom nadzorczym na podstawie art. 58 ust. 2 tego rozporządzenia (zob. analogicznie, w odniesieniu do art. 25 ust. 6 i art. 28 dyrektywy 95/46, wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 102, 103). Wreszcie brzmienie motywu 5 decyzji wykonawczej 2016/2297 potwierdza to, że decyzja w sprawie klauzul standardowych „nie uniemożliwia […] organowi nadzorczemu wykonywania swoich uprawnień w zakresie kontroli przepływów danych, w tym uprawnienia do zawieszenia lub zakazu przekazywania danych osobowych, jeżeli stwierdzi on, że przekazywanie danych odbywa się z naruszeniem unijnych lub krajowych przepisów o ochronie danych”.

116 Należy jednak wyjaśnić, że przysługujące właściwemu organowi nadzorczemu uprawnienia muszą być w pełni wykonywane zgodnie z decyzją, w której Komisja stwierdza, w stosownym przypadku, w zastosowaniu art. 45 ust. 1 zdanie pierwsze RODO, iż określone państwo trzecie zapewnia odpowiedni stopień ochrony. W takim przypadku z art. 45 ust. 1 zdanie drugie tego rozporządzenia w związku z jego motywem 103 wynika bowiem, że przekazywanie danych osobowych do danego państwa trzeciego może mieć miejsce bez potrzeby uzyskania specjalnego zezwolenia.

117 Zgodnie z art. 288 akapit czwarty TFUE wydana przez Komisję decyzja stwierdzająca odpowiedni stopień ochrony jest w całości wiążąca dla wszystkich państw członkowskich, do których została skierowana, a zatem dla wszystkich ich organów w zakresie, w jakim stwierdza ona, że dane państwo trzecie zapewnia odpowiedni stopień ochrony i – efektem tego – dopuszcza takie przekazywanie danych (zob. analogicznie, w odniesieniu do art. 25 ust. 6 dyrektywy 95/46, wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 51 i przytoczone tam orzecznictwo).

118 Dopóki zatem Trybunał nie stwierdzi nieważności decyzji stwierdzającej odpowiedni stopień ochrony, dopóty państwa członkowskie i ich organy, w tym ich niezależne organy nadzorcze, nie mogą przyjmować środków sprzecznych z tą decyzją, takich jak akty zmierzające do stwierdzenia w sposób wiążący, że państwo trzecie, którego dotyczy dana decyzja, nie zapewnia odpowiedniego stopnia ochrony (wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 52 i przytoczone tam orzecznictwo), i w konsekwencji do zawieszenia czy też zakazania przekazywania danych osobowych do tego państwa trzeciego.

119 Niemniej jednak decyzja Komisji przyjęta na podstawie art. 45 ust. 3 RODO nie uniemożliwia osobom, których dane osobowe zostały lub mogły zostać przekazane do państwa trzeciego, wniesienia do właściwego krajowego organu nadzorczego w zastosowaniu art. 77 ust. 1 RODO skargi dotyczącej ochrony ich praw i wolności w związku z przetwarzaniem tych danych. Podobnie decyzja tego rodzaju nie może zanegować ani ograniczyć kompetencji wyraźnie przyznanych krajowym organom

nadzorczym w art. 8 ust. 3 karty oraz w art. 51 ust. 1 i art. 57 ust. 1 lit. a) tego rozporządzenia (zob. analogicznie, w odniesieniu do art. 25 ust. 6 i art. 28 dyrektywy 95/46, wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 53).

120 A zatem nawet w przypadku wydania przez Komisję decyzji stwierdzającej odpowiedni stopień ochrony właściwy krajowy organ nadzorczy, do którego dana osoba wniosła skargę dotyczącą ochrony jej praw i wolności w związku z przetwarzaniem dotyczących jej danych osobowych, powinien mieć możliwość zbadania w sposób całkowicie niezależny tego, czy przekazywanie tych danych spełnia wymogi ustanowione w RODO oraz, w odpowiednim przypadku, wniesienia do sądów krajowych skargi mającej na celu skierowanie przez te sądy, jeśli podzielą one wątpliwości tego organu co do ważności tej decyzji stwierdzającej odpowiedni stopień ochrony, odesłania prejudycjalnego mającego doprowadzić do przeanalizowania tej ważności (zob. analogicznie, w odniesieniu do art. 25 ust. 6 i art. 28 dyrektywy 95/46, wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 57, 65).

121 W świetle powyższych rozważań na pytanie ósme należy odpowiedzieć, że art. 58 ust. 2 lit. f) i j) RODO należy interpretować w ten sposób, że – o ile nie istnieje ważna decyzja Komisji stwierdzająca odpowiedni stopień ochrony danych – właściwy organ nadzorczy jest zobowiązany do zawieszenia lub zakazania przekazywania danych do państwa trzeciego na podstawie standardowych klauzul ochrony danych przyjętych przez Komisję, jeżeli ten organ nadzorczy w świetle całokształtu okoliczności towarzyszących temu przekazywaniu uzna, że klauzule te nie są lub nie mogą być przestrzegane w tym państwie trzecim, a ochrona przekazywanych danych, jakiej wymaga prawo Unii, a w szczególności art. 45 i 46 RODO i karta, nie może być zapewniona za pomocą innych środków, jeśli to przekazywanie danych nie zostało zawieszone lub zakończone przez samego administratora lub podmiot przetwarzający z siedzibą w Unii.

W przedmiocie pytań siódmego i jedenastego

122 W pytaniach siódmym i jedenastym, które należy rozpatrzyć łącznie, sąd odsyłający zwraca się zasadniczo do Trybunału z pytaniem o ważność decyzji w sprawie w sprawie klauzul standardowych w świetle art. 7, 8 i 47 karty.

123 W szczególności, jak wynika z samego brzmienia pytania siódmego i związanych z nim wyjaśnień zawartych we wniosku o wydanie orzeczenia w trybie prejudycjalnym, sąd odsyłający zastanawia się, czy decyzja w sprawie klauzul standardowych jest w stanie zapewnić odpowiedni stopień ochrony danych osobowych przekazywanych do państw trzecich, skoro przewidziane w niej standardowe klauzule ochrony danych nie wiążą organów tych państw trzecich.

124 Artykuł 1 decyzji w sprawie klauzul standardowych stanowi, że standardowe klauzule umowne zawarte w załączniku do niej uważa się za zapewniające odpowiednie gwarancje ochrony prywatności oraz podstawowych praw i wolności osób fizycznych oraz wykonywania odpowiednich praw zgodnie z wymogami art. 26 ust. 2 dyrektywy 95/46. Treść tego przepisu została w istocie powtórzona w art. 46 ust. 1 i w art. 46 ust. 2 lit. c) RODO.

125 Niemniej jednak, choć klauzule te są wiążące dla administratora danych mającego siedzibę w Unii i odbierającego przekazywane dane podmiotu mającego siedzibę w państwie trzecim, w przypadku gdy zawarli oni umowę zawierającą odesłanie do tych klauzul, bezsporne jest, że wspomniane klauzule nie mogą wiązać organów tego państwa trzeciego, ponieważ nie są one stronami zawartej umowy.

126 Choć zatem istnieją sytuacje, w których, w zależności od stanu prawnego i praktyk stosowanych w danym państwie trzecim, podmiot odbierający przekazywane w ten sposób dane jest w stanie zagwarantować ochronę danych, która jest konieczna, na podstawie samych standardowych klauzul ochrony danych, to jednak zachodzą inne sytuacje, w których postanowienia zawarte w tych

klauzulach mogą nie stanowić wystarczającego środka pozwalającego na zapewnienie w praktyce skutecznej ochrony danych osobowych przekazywanych do danego państwa trzeciego. Ma to miejsce w szczególności wówczas, gdy prawo tego państwa trzeciego pozwala organom jego władzy publicznej na ingerencję w prawa osób, których te dane dotyczą.

127 Powstaje zatem pytanie, czy wydana na podstawie art. 46 ust. 2 lit. c) RODO decyzja Komisji dotycząca standardowych klauzul ochrony danych jest nieważna w braku zawarcia w tej decyzji zabezpieczeń egzekwowalnych wobec organów władzy publicznej państw trzecich, do których dane osobowe są lub mogłyby być przekazywane na podstawie tych klauzul.

128 Artykuł 46 ust. 1 RODO stanowi, że w razie braku decyzji stwierdzającej odpowiedni stopień ochrony administrator danych lub podmiot przetwarzający mogą je przekazać do państwa trzeciego wyłącznie wówczas, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej. Zgodnie z art. 46 ust. 2 lit. c) tego rozporządzenia zabezpieczenia te można zapewnić w drodze przyjętych przez Komisję standardowych klauzul ochrony danych. Przepisy te nie stanowią zaś, że wszystkie te zabezpieczenia muszą być przewidziane w decyzji Komisji takiej jak decyzja w sprawie klauzul standardowych.

129 Należy w tym względzie zauważyć, że tego rodzaju decyzja różni się od decyzji wydawanej na podstawie art. 45 ust. 3 RODO stwierdzającej odpowiedni stopień ochrony, która, po tym, jak przeprowadzone zostanie badanie przepisów danego państwa trzeciego, uwzględniające w szczególności właściwe ustawodawstwo w dziedzinie bezpieczeństwa narodowego i dostępu organów władzy publicznej do danych osobowych, ma na celu stwierdzenie ze skutkiem wiążącym, że państwo trzecie, terytorium lub jeden lub kilka z określonych w nim sektorów zapewniają odpowiedni stopień ochrony i że w związku z tym dostęp, jaki mają organy władzy publicznej tego państwa trzeciego do takich danych, nie stoi na przeszkodzie ich przekazywaniu do tego państwa. Taka decyzja stwierdzająca odpowiedni stopień ochrony może zostać przyjęta przez Komisję jedynie pod warunkiem, że instytucja ta stwierdziła, iż właściwe ustawodawstwo tego państwa trzeciego w tej dziedzinie rzeczywiście przewiduje wszystkie wymagane zabezpieczenia pozwalające uznać, że zapewnia ono tę ochronę w odpowiednim stopniu.

130 Natomiast w odniesieniu do decyzji, w której Komisja przyjmuje standardowe klauzule ochrony danych, takiej jak decyzja w sprawie klauzul standardowych, ze względu na to, że taka decyzja nie dotyczy państwa trzeciego, terytorium lub kilku określonych w nim sektorów, z art. 46 ust. 1 i art. 46 ust. 2 lit. c) RODO nie można wyciągnąć wniosku, że Komisja przed wydaniem takiej decyzji jest zobowiązana do przeprowadzenia oceny tego, czy państwa trzecie, do których dane osobowe mogłyby zostać przekazane na podstawie takich klauzul, zapewniają odpowiedni stopień ochrony.

131 W tym względzie należy przypomnieć, że zgodnie z art. 46 ust. 1 tego rozporządzenia w braku wydania przez Komisję decyzji stwierdzającej odpowiedni stopień ochrony mający siedzibę w Unii administrator danych lub podmiot przetwarzający mają obowiązek zapewnienia odpowiednich zabezpieczeń. Motywy 108 i 114 wspomnianego rozporządzenia potwierdzają, że w przypadku gdy Komisja nie zajęła stanowiska w przedmiocie tego, czy zapewniany w państwie trzecim stopień ochrony danych jest odpowiedni, administrator danych lub, gdy ma to zastosowanie, podmiot przetwarzający „powinni zastosować środki rekompensujące brak ochrony danych w państwie trzecim, zapewniając osobie, której dane dotyczą, odpowiednie zabezpieczenia”, zaś „[z]abezpieczenia te powinny zapewniać, by przestrzegane były wymogi ochrony danych oraz prawa osób, których dane dotyczą, takie same jak w przypadku przetwarzania wewnątrzunijnego, w tym zapewniać dostępność egzekwowalnych praw osoby, której dane dotyczą, i skutecznych środków ochrony prawnej […] w Unii lub w państwie trzecim”.

132 Ponieważ, jak wynika z pkt 125 niniejszego wyroku, umowny charakter standardowych klauzul ochrony danych nierozerwalnie wiąże się z tym, że nie mogą one wiązać organów władzy publicznej państw trzecich, zaś w art. 44, art. 46 ust. 1 i art. 46 ust. 2 lit. c) RODO interpretowanych w świetle art. 7, 8 i 47 karty ustanowiony został wymóg, aby nie obniżać zapewnianego tym rozporządzeniem stopnia

ochrony osób fizycznych, może okazać się konieczne uzupełnienie tych zabezpieczeń zawartych w standardowych klauzulach ochrony danych. W tym względzie motyw 109 tego rozporządzenia stanowi, że „[m]ożliwość korzystania przez administratora [danych] ze standardowych klauzul ochrony danych przyjętych przez Komisję lub organ nadzorczy nie powinna stanowić […] przeszkody, by […] dodać inne klauzule lub dodatkowe zabezpieczenia", dodając w szczególności, że podmioty te „[n]ależy zachęcać […], by w drodze zobowiązań umownych przewidywały dodatkowe zabezpieczenia, stanowiące uzupełnienie dla standardowych klauzul ochrony [danych]".

133 Należy zatem uznać, że standardowe klauzule ochrony danych przyjęte przez Komisję na podstawie art. 46 ust. 2 lit. c) tego rozporządzenia mają na celu wyłącznie ustanowienie dla mających siedzibę w Unii administratorów danych lub podmiotów przetwarzających zabezpieczeń umownych znajdujących jednolite zastosowanie we wszystkich państwach trzecich, a zatem niezależnie od stopnia ochrony gwarantowanego w każdym z tych państw. Ze względu na to, że te standardowe klauzule ochrony danych nie mogą, ze względu na swój charakter, przewidywać zabezpieczeń wykraczających poza umowne zobowiązanie do monitorowania przestrzegania stopnia ochrony wymaganego przez prawo Unii, w zależności od sytuacji panującej w danym państwie trzecim mogą one ustanawiać wymóg podjęcia przez administratora danych dodatkowych środków mających na celu zapewnienie przestrzegania tego stopnia ochrony.

134 W tym względzie, jak zauważył Rzecznik generalny w pkt 126 opinii, przewidziany w art. 46 ust. 2 lit. c) RODO mechanizm kontraktowy opiera się na nałożeniu odpowiedzialności na mających siedzibę w Unii administratora danych lub podmiot przetwarzający, a także, pomocniczo, na właściwy organ nadzorczy. W związku z tym to do tego administratora danych lub podmiotu przetwarzającego należy sprawdzenie w każdym konkretnym przypadku i – gdy ma to zastosowanie – we współpracy z podmiotem odbierającym te dane, czy prawo państwa trzeciego przeznaczenia zapewnia właściwą, w świetle prawa Unii, ochronę danych osobowych przekazywanych na podstawie standardowych klauzul ochrony danych, udzielając w razie potrzeby zabezpieczeń dodatkowych w stosunku do tych zapewnianych w tych klauzulach.

135 W przypadku braku możliwości podjęcia przez mających siedzibę w Unii administratora danych lub podmiot przetwarzający dodatkowych środków odpowiednich dla zagwarantowania takiej ochrony, podmioty te lub, pomocniczo, właściwy organ nadzorczy, są zobowiązane do zawieszenia lub zakończenia przekazywania danych osobowych do danego państwa trzeciego. Jest tak w szczególności w przypadku, gdy prawo tego państwa trzeciego nakłada na podmiot odbierający te pochodzące z Unii dane osobowe zobowiązania, które pozostają w sprzeczności z tymi klauzulami i, co za tym idzie, mogą mieć negatywny wpływ na udzielone umownie zabezpieczenie odpowiedniego stopnia ochrony przed dostępem do tych danych ze strony organów władz publicznych tego państwa trzeciego.

136 Tak więc okoliczność polegająca na tym, że zawarte w wydanej przez Komisję na podstawie art. 46 ust. 2 lit. c) RODO decyzji standardowe klauzule ochrony danych, takie jak te zawarte w załączniku do decyzji w sprawie klauzul standardowych, nie wiążą organów władz państw trzecich, do których dane osobowe mogą zostać przekazane, pozostaje sama w sobie bez wpływu na ważność tej decyzji.

137 Ważność ta zależy natomiast od tego, czy zgodnie z wymogiem wynikającym z art. 46 ust. 1 i art. 46 ust. 2 lit. c) RODO, interpretowanym w świetle art. 7, 8 i 47 karty, taka decyzja przewiduje skuteczne mechanizmy umożliwiające w praktyce zapewnienie przestrzegania wymaganego przez prawo Unii stopnia ochrony i czy odbywające się na podstawie takich klauzul przekazywanie danych osobowych zostanie w przypadku ich naruszenia lub niemożności ich przestrzegania zawieszone lub zakazane.

138 Co się tyczy zabezpieczeń przewidzianych w standardowych klauzulach ochrony danych zawartych w załączniku do decyzji w sprawie klauzul standardowych, z klauzuli 4 lit. a) i b), klauzuli 5 lit. a), klauzuli 9, a także z klauzuli 11 ust. 1 wynika, że mający siedzibę w Unii administrator danych, podmiot odbierający dane osobowe oraz ewentualny podmiot przetwarzający zobowiązują się wzajemnie do tego, aby przetwarzanie tych danych, w tym ich przekazywanie, było nadal dokonywane

zgodnie z „właściwym prawem o ochronie danych", które, zgodnie z definicją zawartą w art. 3 lit. f) tej decyzji, oznacza „prawodawstwo chroniące podstawowe prawa i wolności osób fizycznych, a w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych, właściwe dla administratora danych w państwie członkowskim, w którym podmiot przekazujący dane prowadzi działalność gospodarczą". Odczytywane w świetle karty przepisy RODO stanowią zaś część tego prawodawstwa.

139 Ponadto mający siedzibę w państwie trzecim podmiot odbierający dane osobowe zobowiązuje się, zgodnie z tą klauzulą 5 lit. a), do natychmiastowego poinformowania mającego siedzibę w Unii administratora danych o swej ewentualnej niemożności wywiązania się z obowiązków ciążących na nim na mocy zawartej umowy. W szczególności zgodnie ze wspomnianą klauzulą 5 lit. b) odbiorca ten zaświadcza, że nie ma żadnego powodu, by sądzić, iż mające do niego zastosowanie prawodawstwo uniemożliwia mu wywiązanie się z obowiązków ciążących na nim na mocy zawartej umowy i zobowiązuje się do jak najszybszego zawiadomienia administratora danych, po powzięciu o nich wiadomości, o wszelkich dotyczących go zmianach ustawodawstwa krajowego, które mogą mieć istotne negatywne skutki dla zabezpieczeń i obowiązków określonych w standardowych klauzulach ochrony danych znajdujących się w załączniku do decyzji w sprawie klauzul standardowych. Ponadto, choć ta klauzula 5 lit. d) ppkt (i) pozwala podmiotowi odbierającemu dane osobowe w przypadku istnienia ustawodawstwa, które może on powołać na swoją obronę, takiego jak mający karny charakter zakaz mający na celu zachowanie tajemnicy dochodzenia policyjnego, na nieprzekazywanie mającemu siedzibę w Unii administratorowi danych prawnie wiążącego wniosku o ujawnienie danych osobowych ze strony organów ścigania, o tyle jest on jednak zobowiązany, zgodnie z zawartą w załączniku do decyzji w sprawie klauzul standardowych klauzulą 5 lit. a), do poinformowania tego administratora danych o swej niemożności spełnienia tego warunku zgodnie ze standardowymi klauzulami ochrony danych.

140 W obu przedstawionych w niej przypadkach klauzula 5 lit. a) i b) przyznaje mającemu siedzibę w Unii administratorowi danych prawo do zawieszenia przekazywania danych czy też rozwiązania umowy. W świetle wymogów wynikających z art. 46 ust. 1 i art. 46 ust. 2 lit. c) RODO, rozpatrywanych w świetle art. 7 i 8 karty, zawieszenie przekazywania danych lub rozwiązanie umowy są dla administratora danych obowiązkowe, w przypadku gdy podmiot odbierający te dane nie jest lub przestał być w stanie przestrzegać standardowych klauzul ochrony danych. W przeciwnym razie administrator danych dopuszcza się naruszenia wymogów wynikających z zawartej w załączniku do decyzji w sprawie klauzul standardowych klauzuli 4 lit. a) interpretowanych w świetle przepisów zawartych w RODO i w karcie.

141 Okazuje się zatem, że klauzula 4 lit. a) oraz klauzula 5 lit. a) i b) tego załącznika nakładają na mających siedzibę w Unii administratora i podmiot odbierający dane osobowe obowiązek upewnienia się, iż ustawodawstwo państwa trzeciego przeznaczenia daje temu podmiotowi odbierającemu możliwość dostosowania się do standardowych klauzul ochrony danych zawartych w załączniku do decyzji w sprawie klauzul standardowych jeszcze przed przekazaniem tych danych do tego państwa trzeciego. W odniesieniu do tej weryfikacji w przypisie do klauzuli 5 wyjaśniono, że przewidziane w tych przepisach krajowych nadrzędne wymogi niewykraczające poza to, co konieczne w demokratycznym społeczeństwie w celu zabezpieczenia, w szczególności, bezpieczeństwa narodowego, obronności i bezpieczeństwa publicznego nie są sprzeczne ze standardowymi klauzulami ochrony danych. Przeciwnie, jak podkreślił Rzecznik generalny w pkt 131 opinii, zastosowanie się do wynikającego z prawa docelowego państwa trzeciego obowiązku, który wykracza poza to, co jest konieczne w tym celu, należy potraktować jako naruszenie tych klauzul. Dokonywana przez te podmioty ocena konieczności spełnienia takiego obowiązku winna, gdy zachodzi taka potrzeba, uwzględniać stwierdzenie, iż dane państwo trzecie zapewnia odpowiedni stopień ochrony, zawarte przez Komisję w wydanej na podstawie art. 45 ust. 3 RODO decyzji stwierdzającej odpowiedni stopień ochrony.

142 Wynika z tego, że mający siedzibę w Unii administrator i podmiot odbierający dane osobowe mają obowiązek uprzedniego sprawdzenia tego, czy w danym państwie trzecim jest przestrzegany wymagany przez prawo Unii stopień ochrony. Podmiot odbierający te dane jest, gdy zachodzi taka potrzeba, zobowiązany na mocy tej samej klauzuli 5 lit. b) do poinformowania administratora danych o swej ewentualnej niemożności zastosowania się do tych klauzul, w którym to przypadku to do niego należy zawieszenie przekazywania danych lub rozwiązanie umowy.

143 Jeżeli podmiot odbierający dane osobowe przekazywane do państwa trzeciego powiadomił administratora na podstawie klauzuli 5 lit. b) załącznika do decyzji w sprawie klauzul standardowych, że ustawodawstwo danego państwa trzeciego nie pozwala mu zastosować się do zawartych w tym załączniku standardowych klauzul ochrony danych, to z klauzuli 12 tego załącznika wynika, że dane, które zostały już przekazane do tego państwa trzeciego, oraz ich kopie powinny zostać w całości zwrócone lub zniszczone. W każdym razie klauzula 6 tego samego załącznika przewiduje sankcję za uchybienie tym standardowym klauzulom, przyznając osobie, której dane dotyczą, prawo do uzyskania odszkodowania za poniesioną szkodę.

144 Należy dodać, że zgodnie z klauzulą 4 lit. f) załącznika do decyzji w sprawie klauzul standardowych, w sytuacji gdy dane mogłyby zostać przekazane do państwa trzeciego, które nie zapewnia odpowiedniej ochrony, mający siedzibę w Unii administrator zobowiązuje się do poinformowania o tym osoby, której dane dotyczą, jeszcze przed przekazaniem lub jak najszybciej po nim. Informacja ta może umożliwić tej osobie skorzystanie z przyznanego jej na mocy klauzuli 3 ust. 1 prawa do wniesienia przeciwko administratorowi skargi o zawieszenie planowanego przekazania, rozwiązanie umowy zawartej z podmiotem odbierającym dane osobowe lub, gdy zachodzi taka konieczność, zażądanie od niego zwrotu lub zniszczenia przekazanych danych.

145 Wreszcie, zgodnie z klauzulą 4 lit. g) tego załącznika, w przypadku gdy podmiot odbierający dane osobowe na podstawie klauzuli 5 lit. b) powiadomi mającego siedzibę w Unii administratora, że dotyczące go ustawodawstwo zostało zmienione w sposób, który może mieć istotne negatywne skutki dla zabezpieczeń i obowiązków określonych w standardowych klauzulach ochrony danych, administrator ten jest zobowiązany do przekazania tego powiadomienia do właściwego organu nadzorczego, jeśli, pomimo otrzymania tego powiadomienia, zdecyduje się on kontynuować przekazywanie danych lub znieść jego zawieszenie. Przekazanie takiego powiadomienia temu organowi nadzorczemu i przysługujące temu organowi prawo do przeprowadzenia kontroli u podmiotu odbierającego dane osobowe na podstawie klauzuli 8 ust. 2 tego samego załącznika umożliwiają temu organowi sprawdzenie, czy w celu zapewnienia odpowiedniego stopnia ochrony należy dokonać zawieszenia lub ustanowić zakaz planowanego przekazywania danych osobowych.

146 W tym kontekście art. 4 decyzji w sprawie klauzul standardowych] w związku z motywem 5 decyzji wykonawczej 2016/2297 potwierdza, że decyzja w sprawie w sprawie klauzul standardowych w żaden sposób nie uniemożliwia właściwemu organowi nadzorczemu zawieszenia lub zakazania, gdy zachodzi taka konieczność, przekazywania danych osobowych do państwa trzeciego na podstawie zawartych w załączniku do tej decyzji standardowych klauzul ochrony danych. W tym względzie, jak wynika z odpowiedzi na pytanie ósme, jeżeli nie istnieje ważnie przyjęta przez Komisję decyzja stwierdzająca odpowiedni stopień ochrony, właściwy organ nadzorczy jest zobowiązany na podstawie art. 58 ust. 2 lit. f) i j) RODO do zawieszenia lub zakazania przekazywania danych osobowych do państwa trzeciego, jeżeli w świetle wszystkich okoliczności towarzyszących temu przekazywaniu stwierdzi, że te klauzule nie są lub nie mogą być przestrzegane w tym państwie trzecim i że nie można zapewnić wymaganej przez unijne prawo ochrony przekazywanych danych przy pomocy innych środków, jeśli to przekazywanie nie zostało zawieszone lub zakończone przez samego administratora lub podmiot przetwarzający z siedzibą w Unii.

147 Jeśli chodzi o podniesioną przez komisarza okoliczność polegającą na tym, że przekazywanie danych osobowych do takiego państwa trzeciego mogłoby ewentualnie być przedmiotem przyjmowanych przez organy nadzorcze w różnych państwach członkowskich rozbieżnych decyzji, należy dodać, że,

jak wynika z art. 55 ust. 1 i art. 57 ust. 1 lit. a) RODO, zadanie czuwania nad przestrzeganiem tego rozporządzenia zostało powierzone co do zasady organowi nadzorczemu właściwemu na terytorium danego państwa członkowskiego. Ponadto, w celu uniknięcia wydawania rozbieżnych decyzji, art. 64 ust. 2 tego rozporządzenia przewiduje możliwość zwrócenia się przez taki organ nadzorczy, który uważa, że przekazywanie danych do danego państwa trzeciego winno być ogólnie zakazane, do Europejskiej Rady Ochrony Danych (EROD), która na podstawie art. 65 ust. 1 lit. c) tego samego rozporządzenia może wydać wiążącą decyzję, w szczególności gdy organ nadzorczy nie stosuje się do wydanej opinii.

148 Wynika z tego, że decyzja w sprawie klauzul standardowych przewiduje skuteczne mechanizmy umożliwiające w praktyce zapewnienie, iż przekazywanie do państwa trzeciego danych osobowych na podstawie zawartych w załączniku do tej decyzji standardowych klauzul ochrony danych zostanie zawieszone lub zakazane, jeżeli podmiot odbierający dane nie przestrzega tych klauzul lub nie jest w stanie ich przestrzegać.

149 W świetle całości powyższych rozważań na pytania siódme i jedenaste należy odpowiedzieć, że badanie decyzji w sprawie klauzul standardowych w świetle art. 7, 8 i 47 karty nie doprowadziło do żadnych ustaleń, które mogłyby mieć wpływ na ważność tej decyzji.

W przedmiocie pytań czwartego, piątego, dziewiątego i dziesiątego

150 Poprzez pytanie dziewiąte sąd odsyłający dąży zasadniczo do ustalenia, czy i w jakim zakresie organ nadzorczy państwa członkowskiego jest związany zawartymi w decyzji w sprawie Tarczy Prywatności ustaleniami, zgodnie z którymi Stany Zjednoczone zapewniają odpowiedni stopień ochrony. W pytaniach czwartym, piątym i dziesiątym sąd ten zmierza zasadniczo do ustalenia, czy – biorąc pod uwagę jego własne ustalenia dotyczące prawa Stanów Zjednoczonych – przekazywanie do tego państwa trzeciego danych osobowych na podstawie standardowych klauzul ochrony danych zawartych w załączniku do decyzji w sprawie klauzul standardowych narusza prawa zagwarantowane w art. 7, 8 i 47 karty, i zwraca się do Trybunału w szczególności o wyjaśnienie, czy powołanie Rzecznika, o którym mowa w załączniku III do decyzji w sprawie Tarczy Prywatności, jest zgodne z tym art. 47.

151 Na wstępie należy zauważyć, że choć we wniesionej przezeń w postępowaniu głównym skardze komisarz podaje w wątpliwość jedynie ważność decyzji w sprawie klauzul standardowych, skarga ta została wniesiona do sądu odsyłającego jeszcze przed wydaniem decyzji w sprawie Tarczy Prywatności. W zakresie, w jakim zadając pytania czwarte i piąte, sąd ten zwraca się do Trybunału w sposób ogólny o wyjaśnienie ochrony, jaką należy zapewnić na mocy art. 7, 8 i 47 karty w kontekście takiego przekazania, przeprowadzane przez Trybunał badanie powinno uwzględniać konsekwencje wynikające z wydania w międzyczasie decyzji w sprawie Tarczy Prywatności. Jest tak, tym bardziej że wspomniany sąd w pytaniu dziesiątym wyraźnie pyta, czy ochrona wymagana przez art. 47 jest zapewniana dzięki Rzecznikowi, o którym mowa w tej ostatniej decyzji.

152 Ponadto z informacji zawartych we wniosku o wydanie orzeczenia w trybie prejudycjalnym wynika, że w ramach postępowania głównego Facebook Ireland podniosła, iż decyzja w sprawie Tarczy Prywatności wywołuje wobec komisarza wiążące skutki w zakresie stwierdzenia zapewnianego przez Stany Zjednoczone odpowiedniego stopnia ochrony i w konsekwencji co do zgodności z prawem przekazywania do tego państwa trzeciego danych osobowych na podstawie standardowych klauzul ochrony danych zawartych w załączniku do decyzji w sprawie klauzul standardowych.

153 Jak zaś wynika z pkt 59 niniejszego wyroku, w załączonym do wniosku o wydanie orzeczenia w trybie prejudycjalnym wyroku z dnia 3 października 2017 r. sąd odsyłający podkreślił, że jest zobowiązany do uwzględnienia ewentualnych zmian przepisów prawa, jakie zaszły w okresie pomiędzy wniesieniem skargi a przeprowadzoną przed nim rozprawą. Tym samym sąd ten wydaje się być w obowiązku

uwzględnić przy rozstrzyganiu sporu zawisłego w postępowaniu głównym zmiany okoliczności, jaka zaszła wskutek wydania decyzji w sprawie Tarczy Prywatności, a także ewentualnych wiążących skutków tego rozstrzygnięcia.

154 W szczególności istnienie wiążących skutków związanych ze stwierdzeniem w decyzji w sprawie Tarczy Prywatności zapewnianego w Stanach Zjednoczonych odpowiedniego stopnia ochrony jest istotne dla celów oceny zarówno przypomnianych w pkt 141 i 142 niniejszego wyroku obowiązków spoczywających na administratorze i na podmiocie odbierającym dane osobowe przekazywane do państwa trzeciego na podstawie standardowych klauzul ochrony danych zawartych w załączniku do decyzji w sprawie klauzul standardowych, jak i spoczywających na organie nadzorczym obowiązków zawieszenia lub zakazania takiego przekazania, gdy zachodzi taka konieczność.

155 W odniesieniu do wiążących skutków decyzji w sprawie Tarczy Prywatności art. 1 ust. 1 tej decyzji stanowi, że do celów art. 45 ust. 1 RODO „Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do podmiotów w Stanach Zjednoczonych w ramach Tarczy Prywatności [Unia Europejska]–USA". Zgodnie z art. 1 ust. 3 wspomnianej decyzji dane osobowe są uważane za przekazywane w ramach Tarczy Prywatności, w przypadku gdy przekazuje się je z Unii do podmiotów w Stanach Zjednoczonych, które figurują w wykazie podmiotów uczestniczących w programie Tarczy prowadzonym i udostępnianym publicznie przez departament handlu Stanów Zjednoczonych zgodnie z sekcjami I i III zasad przedstawionych w załączniku II do tej decyzji.

156 Jak wynika z orzecznictwa przypomnianego w pkt 117 i 118 niniejszego wyroku, decyzja w sprawie Tarczy Prywatności ma charakter wiążący dla organów nadzorczych w zakresie, w jakim stwierdza, że Stany Zjednoczone gwarantują odpowiedni stopień ochrony, i, co za tym idzie, skutkuje upoważnieniem do przekazywania danych osobowych w ramach Tarczy Prywatności Unia Europejska–USA. W związku z tym, dopóki Trybunał nie stwierdzi nieważności tej decyzji, właściwy organ nadzorczy nie może zawiesić lub zakazać przekazywania danych osobowych podmiotowi uczestniczącemu w Tarczy Prywatności ze względu na to, że wbrew ocenie przyjętej przez Komisję we wspomnianej decyzji uważa on, że ustawodawstwo Stanów Zjednoczonych regulujące dostęp do danych osobowych przekazywanych w ramach Tarczy Prywatności i ich wykorzystywanie przez organy władzy publicznej tego państwa trzeciego do celów bezpieczeństwa narodowego, egzekwowania prawa i innych celów leżących w interesie publicznym nie zapewnia tej ochrony w odpowiednim stopniu.

157 Niemniej jednak zgodnie z orzecznictwem przypomnianym w pkt 119 i 120 niniejszego wyroku właściwy organ nadzorczy, do którego dana osoba wniosła skargę, powinien zbadać w sposób całkowicie niezależny, czy przekazanie danych tej osoby spełnia wymogi ustanowione w RODO, i w przypadku gdy uzna zarzuty podniesione przez tę osobę w celu podważenia ważności decyzji stwierdzającej odpowiedni stopień ochrony za zasadne, wnieść do sądu krajowego skargę zmierzającą do zwrócenia się przezeń do Trybunału z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w przedmiocie oceny ważności tej decyzji.

158 Wniesioną na podstawie art. 77 ust. 1 RODO skargę, w której osoba, której dane osobowe zostały lub mogły zostać przekazane do państwa trzeciego, podnosi, że prawo i praktyki danego państwa trzeciego nie zapewniają, niezależnie od ustaleń poczynionych przez Komisję w decyzji przyjętej na podstawie art. 45 ust. 3 tego rozporządzenia, odpowiedniego stopnia ochrony, należy bowiem rozumieć jako dotyczącą w istocie zgodności tej decyzji z ochroną życia prywatnego oraz wolności i praw podstawowych jednostek (zob. analogicznie, w odniesieniu do art. 25 ust. 6 i art. 28 ust. 4 dyrektywy 95/46, wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 59).

159 W niniejszej sprawie M. Schrems zwrócił się do komisarza zasadniczo o zakazanie lub zawieszenie przekazywania przez Facebook Ireland jego danych osobowych spółce Facebook Inc. z siedzibą w Stanach Zjednoczonych ze względu na to, że to państwo trzecie nie zapewnia odpowiedniego stopnia ochrony. Ponieważ komisarz po przeprowadzeniu dochodzenia w przedmiocie podnoszonych przez

M. Schremsa zarzutów zwrócił się do sądu odsyłającego, sąd ten wydaje się, w świetle przedstawionych dowodów i przeprowadzonej przed nim kontradyktoryjnej debaty, zastanawiać nad zasadnością wątpliwości żywionych przez M. Schremsa –co stwierdziła w międzyczasie Komisja w decyzji w sprawie Tarczy Prywatności – dotyczących zapewnianego w tym państwie trzecim odpowiedniego stopnia ochrony, co skłoniło ten sąd do skierowania do Trybunału pytań prejudycjalnych czwartego, piątego i dziesiątego.

160 Jak zauważył Rzecznik generalny w pkt 175 opinii, te pytania prejudycjalne należy rozumieć w ten sposób, że dotyczą one w istocie zawartego w decyzji w sprawie Tarczy Prywatności stwierdzenia Komisji, zgodnie z którym Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do tego państwa trzeciego, a tym samym – ważności tej decyzji.

161 Uwzględniając okoliczności wskazane w pkt 121 i 157–160 niniejszego wyroku i w celu udzielenia sądowi odsyłającemu odpowiedzi w pełnym zakresie, należy zbadać, czy decyzja w sprawie Tarczy Prywatności jest zgodna z wymogami wynikającymi z RODO w związku z kartą (zob. analogicznie wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 67).

162 Przyjęcie przez Komisję decyzji na podstawie art. 45 ust. 3 RODO wymaga prawidłowo uzasadnionego ustalenia przez tę instytucję, że dane państwo trzecie rzeczywiście zapewnia, ze względu na swoje ustawodawstwo wewnętrzne i zobowiązania międzynarodowe, stopień ochrony praw podstawowych merytorycznie równoważny temu gwarantowanemu w unijnym porządku prawnym (zob. analogicznie w odniesieniu do art. 25 ust. 6 dyrektywy 95/46 wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 96).

W przedmiocie treści decyzji w sprawie Tarczy Prywatności

163 Komisja w art. 1 ust. 1 decyzji w sprawie Tarczy Prywatności stwierdziła, że Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do podmiotów w Stanach Zjednoczonych w ramach Tarczy Prywatności Unia Europejska–USA, na którą składają się w szczególności, zgodnie z art. 1 ust. 2 tej decyzji, zasady wydane przez departament handlu Stanów Zjednoczonych w dniu 7 lipca 2016 r., wskazane w załączniku II, oraz oficjalne oświadczenia i zobowiązania zawarte w dokumentach przedstawionych w załącznikach I i III–VII do tej decyzji.

164 Jednakże w decyzji w sprawie Tarczy Prywatności, a konkretnie w pkt I.5 załącznika II do niej, zatytułowanym „Ramowe zasady Tarczy Prywatności [Unia Europejska]–USA”, wyjaśniono również, że przestrzeganie tych zasad może być ograniczone między innymi „w zakresie niezbędnym do spełnienia wymagań bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa”. Podobnie jak w decyzji 2000/520, w decyzji w sprawie Tarczy Prywatności ustanowione zostało pierwszeństwo tych wymogów przed tymi zasadami, pierwszeństwo, na mocy którego otrzymujące dane osobowe z Unii amerykańskie organizacje, które dokonały samocertyfikacji, zobowiązane są odstąpić bez wyjątku od tych zasad, jeśli pozostają one w konflikcie z tymi wymogami i okazują się w związku z tym z nimi niezgodne (zob. analogicznie w odniesieniu do decyzji 2000/520 wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 86).

165 Ze względu na swój ogólny charakter odstępstwo ustanowione w pkt I.5 załącznika II do decyzji w sprawie Tarczy Prywatności umożliwia w ten sposób ingerencje – oparte na wymaganiach bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa – w prawa podstawowe osób, których dane osobowe są przekazywane lub mogłyby zostać przekazane z Unii do Stanów Zjednoczonych (zob. analogicznie w zakresie dotyczącym decyzji 2000/520 wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 87). W szczególności, jak stwierdzono w decyzji w sprawie Tarczy Prywatności, takie ingerencje mogą wynikać z dostępu do danych

osobowych przekazywanych z Unii do Stanów Zjednoczonych i z wykorzystywania tych danych przez organy amerykańskich władz publicznych w ramach opartych na art. 702 FISA programów nadzoru PRISM i UPSTREAM, a także na podstawie rozporządzenia wykonawczego nr 12333.

166 W tym kontekście w motywach 67–135 decyzji w sprawie Tarczy Prywatności Komisja dokonała oceny ograniczeń i gwarancji przewidzianych w ustawodawstwie Stanów Zjednoczonych, a w szczególności w art. 702 FISA, w rozporządzeniu wykonawczym nr 12333 i w PPD-28, jeśli chodzi o dostęp do danych osobowych przekazywanych w ramach Tarczy Prywatności Unia Europejska–USA i korzystania przez amerykańskie organy publiczne z tych danych do celów bezpieczeństwa narodowego, egzekwowania prawa i innych celów leżących w interesie publicznym.

167 Po przeprowadzeniu tej oceny Komisja w motywie 136 tej decyzji uznała, że „Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do samocertyfikowanych podmiotów w Stanach Zjednoczonych", a w jej motywie 140 stwierdziła, że „na podstawie dostępnych informacji na temat amerykańskiego porządku prawnego, […] wszelkie ingerencje amerykańskich organów publicznych w prawa podstawowe osób, których dane osobowe są przekazywane z Unii do Stanów Zjednoczonych w ramach Tarczy Prywatności UE–USA do celów bezpieczeństwa narodowego, egzekwowania prawa lub innych celów interesu publicznego, a także wiążące się z nimi ograniczenia nałożone na samocertyfikowane podmioty w odniesieniu do przestrzegania przez nie zasad, będą ograniczać się do tego, co jest ściśle niezbędne, aby osiągnąć dany uzasadniony cel, oraz że istnieje skuteczna ochrona prawna przed taką ingerencją".

W przedmiocie stwierdzenia dotyczącego odpowiedniego stopnia ochrony

168 Mając na względzie okoliczności wskazane przez Komisję w decyzji w sprawie Tarczy Prywatności oraz te ustalone przez sąd odsyłający w ramach postępowania głównego, sąd ten ma wątpliwości co do tego, czy prawo Stanów Zjednoczonych zapewnia rzeczywiście stopień ochrony wymagany w art. 45 RODO w związku z prawami podstawowymi gwarantowanymi w art. 7, 8 i 47 karty. W szczególności ten sąd uważa, że prawo tego państwa trzeciego nie przewiduje niezbędnych ograniczeń i zabezpieczeń w odniesieniu do ingerencji dozwolonych w przepisach krajowych ani nie zapewnia skutecznej ochrony sądowej przed tego rodzaju ingerencjami. W tym ostatnim względzie dodaje on, że ustanowienie Rzecznika ds. Tarczy Prywatności nie może jego zdaniem zaradzić tym brakom, ponieważ nie można utożsamiać tego Rzecznika z sądem w rozumieniu art. 47 karty.

169 Co się tyczy w pierwszej kolejności art. 7 i 8 karty, będących częścią regulacji wymaganego w Unii stopnia ochrony i których przestrzeganie musi zostać stwierdzone przez Komisję, zanim instytucja ta wyda na podstawie art. 45 ust. 1 RODO decyzję stwierdzającą odpowiedni stopień ochrony, należy przypomnieć, że art. 7 karty gwarantuje każdej osobie prawo do poszanowania jej życia prywatnego i rodzinnego, domu i komunikowania się. W art. 8 ust. 1 karty wyraźnie zaś przyznano każdemu prawo do ochrony danych osobowych, które go dotyczą.

170 Dostęp do danych osobowych osoby fizycznej w celu ich zatrzymywania lub wykorzystywania narusza zatem przysługujące tej osobie prawo podstawowe do poszanowania życia prywatnego, zagwarantowane w art. 7 karty, przy czym prawo to odnosi się do wszelkich informacji dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Te przypadki przetwarzania danych wchodzą również w zakres zastosowania art. 8 karty z tego powodu, że stanowią przetwarzanie danych osobowych w rozumieniu tego artykułu i w związku z tym muszą spełniać wynikające z niego wymogi w zakresie ochrony danych [zob. podobnie wyroki: z dnia 9 listopada 2010 r., Volker und Markus Schecke i Eifert, C-92/09 i C-93/09, EU:C:2010:662, pkt 49 i 52; a także z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 29; a także opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 122, 123].

171 Trybunał miał już sposobność orzec, że udostępnianie danych osobowych podmiotowi trzeciemu, takiemu jak organ władzy publicznej, stanowi ingerencję w zagwarantowane w art. 7 i 8 karty prawa podstawowe niezależnie od tego, w jaki sposób te dane zostaną później wykorzystane. To samo dotyczy zatrzymywania danych osobowych oraz udzielania do nich dostępu w celu ich wykorzystania przez organy władzy publicznej niezależnie od tego, czy informacje dotyczące życia prywatnego mają charakter wrażliwy i bez względu na to, czy z powodu tej ingerencji zainteresowane osoby doświadczyły ewentualnych niedogodności [zob. podobnie wyroki: z dnia 20 maja 2003 r., Österreichischer Rundfunk i in., C-465/00, C-138/01 i C-139/01, EU:C:2003:294, pkt 74 i 75; a także z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 33–36; a także opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 124, 126].

172 Niemniej jednak praw zagwarantowanych w art. 7 i 8 karty nie sposób uznać za stanowiące prerogatywy o charakterze absolutnym, lecz powinny być one oceniane w świetle ich funkcji społecznej [zob. podobnie wyroki: z dnia 9 listopada 2010 r., Volker und Markus Schecke i Eifert, C-92/09 i C-93/09, EU:C:2010:662, pkt 48 i przytoczone tam orzecznictwo; z dnia 17 października 2013 r., Schwarz, C-291/12, EU:C:2013:670, pkt 33 i przytoczone tam orzecznictwo; a także opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 136].

173 W tym względzie należy również wskazać, że zgodnie z art. 8 ust. 2 karty dane osobowe powinny w szczególności być przetwarzane „w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą”.

174 Ponadto, zgodnie z art. 52 ust. 1 zdanie pierwsze karty wszystkie ograniczenia w korzystaniu z praw i wolności uznanych w karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Zgodnie z art. 52 ust. 1 zdanie drugie karty, z zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

175 W tej ostatniej kwestii należy dodać, że wymóg, zgodnie z którym wszelkie ograniczenia korzystania z praw podstawowych muszą być przewidziane ustawą, oznacza, że podstawa prawna, która pozwala na ingerencję w te prawa, musi sama określać zakres ograniczenia wykonywania danego prawa [zob. w szczególności opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 139 i przytoczone tam orzecznictwo].

176 Wreszcie dane uregulowanie prowadzące do ingerencji – aby spełnić wymóg proporcjonalności, zgodnie z którym odstępstwa od ochrony danych osobowych i jej ograniczeń mogą być stosowane jedynie wtedy, gdy jest to absolutnie konieczne – powinno zawierać jasne i precyzyjne reguły dotyczące zakresu i stosowania rozpatrywanego środka oraz ustanawiać minimalne wymagania służące temu, aby osoby, których dane osobowe zostały przekazane, były zaopatrzone w wystarczające zabezpieczenia umożliwiające rzeczywistą ochronę ich danych przed ryzykiem nadużyć. Powinno ono w szczególności wskazywać, w jakich okolicznościach i pod jakimi warunkami może zostać przyjęty środek przewidujący przetwarzanie takich danych, gwarantując w ten sposób, że ingerencja będzie ograniczona do tego, co ściśle konieczne. Konieczność zaopatrzenia w takie gwarancje jest istotna jeszcze bardziej wówczas, gdy dane osobowe są przetwarzane w sposób zautomatyzowany [zob. podobnie opinia 1/15 (umowa UE–Kanada o danych PNR) z dnia 26 lipca 2017 r., EU:C:2017:592, pkt 140, 141 i przytoczone tam orzecznictwo].

177 W tym celu w art. 45 ust. 2 lit. a) RODO wyjaśniono, że w ramach oceny zapewnianego przez państwo trzecie odpowiedniego stopnia ochrony Komisja bierze pod uwagę w szczególności „istnienie skutecznych i egzekwowalnych praw osób”, których dane osobowe są przekazywane.

178 W niniejszym przypadku dokonane przez Komisję w decyzji w sprawie Tarczy Prywatności stwierdzenie, zgodnie z którym Stany Zjednoczone zapewniają stopień ochrony merytorycznie równoważny temu, który jest gwarantowany w Unii przez RODO w związku z art. 7 i 8 karty, zostało zakwestionowane między innymi ze względu na to, że ingerencje wynikające z programów nadzoru opierających się na art. 702 FISA i rozporządzeniu wykonawczym nr 12333 nie podlegają wymogom, dzięki którym, w poszanowaniu zasady proporcjonalności, zapewniany byłby stopień ochrony merytorycznie równoważny temu zagwarantowanemu w art. 52 ust. 1 karty. Należy zatem zbadać, czy owe programy nadzoru są wdrażane z poszanowaniem takich wymogów, bez konieczności uprzedniego sprawdzania tego, czy w tym państwie trzecim przestrzegane są warunki merytorycznie równoważne tym przewidzianym w art. 52 ust. 1 zdanie pierwsze karty.

179 W tym względzie, jeśli chodzi o programy nadzoru oparte na art. 702 FISA, Komisja w motywie 109 decyzji w sprawie Tarczy Prywatności stwierdziła, że zgodnie z tym artykułem „[FISC] nie jest uprawniony do zatwierdzania poszczególnych środków nadzoru; może jednak zatwierdzać programy nadzoru (takie jak PRISM, UPSTREAM) w oparciu o roczne certyfikacje przygotowywane przez prokuratora generalnego i dyrektora krajowych służb wywiadowczych [DNI]”. Jak wynika z tego motywu, kontrola sprawowana przez FISC ma zatem na celu sprawdzenie, czy te programy nadzoru są odpowiednie do realizacji celu polegającego na pozyskiwaniu zagranicznych informacji wywiadowczych, lecz nie dotyczy kwestii tego, „czy osoby fizyczne są odpowiednio namierzane do celów pozyskiwania zagranicznych informacji wywiadowczych”.

180 Okazuje się zatem, że z art. 702 FISA nie można w żaden sposób wyprowadzić wniosku o istnieniu jakichś ograniczeń ustanowionego w nim uprawnienia odnoszącego się do wdrażania programów nadzoru do celów wywiadu zagranicznego, ani też gwarancji przysługujących potencjalnie objętym tymi programami osobom nieposiadającym obywatelstwa amerykańskiego. W tych okolicznościach i jak zauważył zasadniczo Rzecznik generalny w pkt 291, 292 i 297 opinii, za pomocą tego uregulowania nie można zapewnić stopnia ochrony merytorycznie równoważnego temu gwarantowanemu w karcie w wykładni przyjętej w orzecznictwie przypomnianym w pkt 175 i 176 niniejszego wyroku, zgodnie z którą podstawa prawna umożliwiająca ingerencje w prawa podstawowe powinna – aby spełniać wymóg proporcjonalności – sama określić zakres ograniczenia wykonywania danego prawa oraz przewidywać jasne i precyzyjne zasady dotyczące zakresu i stosowania danego środka oraz ustanawiać pewne wymogi minimalne.

181 Zgodnie z ustaleniami zawartymi w decyzji w sprawie Tarczy Prywatności programy nadzoru mające za podstawę art. 702 FISA powinny niewątpliwie być wdrażane z poszanowaniem wymogów wynikających z PPD-28. Chociaż Komisja podkreśliła w motywach 69 i 77 decyzji w sprawie Tarczy Prywatności, że tego rodzaju wymogi mają dla organów amerykańskich służb wywiadowczych wiążący charakter, rząd amerykański w odpowiedzi na pytanie Trybunału przyznał, że PPD-28 nie przyznaje zainteresowanym osobom, których dane są przekazywane, praw, które mogłyby być egzekwowalne wobec władz amerykańskich przed sądami. Nie można zatem za jego pomocą zapewnić stopnia ochrony merytorycznie równoważnego temu wynikającemu z karty – wbrew wymogowi ustanowionemu w art. 45 ust. 2 lit. a) RODO, zgodnie z którym ocena, czy stopień ten jest odpowiedni, zależy w szczególności od istnienia skutecznych i egzekwowalnych praw osób, których dane są przekazywane do danego państwa trzeciego.

182 Co się tyczy programów nadzoru mających podstawę w rozporządzeniu wykonawczym nr 12333, z akt sprawy, którymi dysponuje Trybunał, wynika, że akt ten również nie przyznaje praw, które mogłyby być egzekwowalne wobec władz amerykańskich przed sądami.

183 Należy dodać, że PPD-28, którego należy przestrzegać w ramach stosowania programów, o których mowa w dwóch poprzednich punktach, umożliwia „»hurtowe« gromadzenie […] względnie dużego wolumenu informacji lub danych gromadzonych w wyniku rozpoznania radioelektronicznego, w sytuacji gdy Wspólnota Wywiadowcza nie może stosować identyfikatora związanego z namierzaną osobą […], by skupić gromadzenie danych na konkretnych celach”, jak zostało to wyjaśnione w piśmie

z dnia 21 czerwca 2016 r., które zostało skierowane przez urząd dyrektora krajowych służb wywiadowczych (Office of the Director of National Intelligence) do departamentu handlu USA oraz do urzędu ds. handlu międzynarodowego, zawartym w załączniku VI do decyzji w sprawie Tarczy Prywatności. Możliwość ta, która oznacza w ramach programów nadzoru mających podstawę w rozporządzeniu wykonawczym nr 12333 udzielenie dostępu do danych, które są „w tranzycie" w kierunku terytorium Stanów Zjednoczonych, przy czym dostęp ten nie jest przedmiotem jakiegokolwiek nadzoru sądowego, w żadnym razie nie stanowi uregulowania w sposób wystarczająco jasny i precyzyjny zakresu takiego „hurtowego" gromadzenia danych osobowych.

184 Należy zatem uznać, że ani art. 702 FISA, ani rozporządzenie wykonawcze nr 12333 w związku z PPD-28 nie odpowiadają wymogom minimalnym związanym w prawie Unii z zasadą proporcjonalności, wobec czego nie można uznać, że programy oparte na tych przepisach nadzoru są ograniczone do tego, co ściśle konieczne.

185 W tych okolicznościach te ograniczenia ochrony danych osobowych, które wynikają z wewnętrznych regulacji Stanów Zjednoczonych dotyczących dostępu i wykorzystywania przez organy amerykańskich władz publicznych takich przekazywanych z Unii do Stanów Zjednoczonych danych, poddanych przez Komisję ocenie w decyzji w sprawie Tarczy Prywatności, nie stanowi uregulowania tych ograniczeń w sposób odpowiadający wymogom merytorycznie równoważnym tym ustanowionym w prawie Unii w art. 52 ust. 1 zdanie drugie karty.

186 Co się tyczy w drugiej kolejności art. 47 karty, który również przyczynia się do wypracowania wymaganego w Unii stopnia ochrony i którego poszanowanie Komisja musi stwierdzić, zanim wyda na podstawie art. 45 ust. 1 RODO decyzję stwierdzającą odpowiedni stopień ochrony, należy przypomnieć, że w akapicie pierwszym tego art. 47 został ustanowiony wymóg, by każdy, kogo prawa i wolności zagwarantowane przez prawo Unii zostały naruszone, miał prawo do skutecznego środka prawnego przed sądem, zgodnie z warunkami przewidzianymi w tym artykule. Zgodnie z akapitem drugim tego artykułu każdy ma prawo do rozpatrzenia jego sprawy przez niezawisły i bezstronny sąd.

187 Zgodnie z utrwalonym orzecznictwem samo istnienie skutecznej kontroli sądowej służącej zapewnieniu poszanowania przepisów prawa Unii jest nierozerwalnie związane z istnieniem państwa prawa. Tak więc uregulowanie nieprzewidujące dla jednostek żadnej drogi prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania czy usunięcia takich danych nie zapewnia poszanowania zasadniczej istoty prawa podstawowego do skutecznej ochrony prawnej, wynikającego z art. 47 karty (wyrok z dnia 6 października 2015 r., Schrems, C-362/14, EU:C:2015:650, pkt 95 i przytoczone tam orzecznictwo).

188 W tym celu w art. 45 ust. 2 lit. a) RODO został ustanowiony wymóg, aby w ramach oceny tego, czy dane państwo trzecie zapewnia odpowiedni stopień ochrony, Komisja brała pod uwagę w szczególności „prawa osób, których dane dotyczą, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia". W motywie 104 RODO podkreśla się w tym względzie, że państwo trzecie „powinno w szczególności zapewnić skuteczny niezależny nadzór nad ochroną danych oraz powinno przewidzieć mechanizmy współpracy z organami ochrony danych państw członkowskich", wyjaśniając, że „osoby, których dane dotyczą, powinny uzyskać skuteczne i egzekwowalne prawa oraz skuteczne administracyjne i sądowe środki zaskarżenia".

189 Istnienie takich skutecznych możliwości zaskarżenia w danym państwie trzecim ma szczególne znaczenie w kontekście przekazywania danych osobowych do tego państwa trzeciego, ponieważ – jak wynika z motywu 116 RODO – osoby, których te dane dotyczą, mogą stanąć w obliczu braku istnienia po stronie organów administracyjnych i sądowych państw członkowskich uprawnień i środków wystarczających do skutecznego nadania biegu ich skargom, w których podnoszą one niezgodne z prawem przetwarzanie w tym państwie trzecim przekazanych w ten sposób danych, co może zmuszać je do zwrócenia się do władz administracyjnych i sądowych tego państwa trzeciego.

190 W niniejszym przypadku dokonane przez Komisję w decyzji w sprawie Tarczy Prywatności ustalenie, zgodnie z którym Stany Zjednoczone zapewniają stopień ochrony merytorycznie równoważny temu gwarantowanemu w art. 47 karty, zostało zakwestionowane w szczególności ze względu na to, że ustanowienie Rzecznika ds. Tarczy Prywatności nie jest w stanie zaradzić stwierdzonym przez samą Komisję brakom w zakresie ochrony sądowej osób, których dane osobowe są przekazywane do tego państwa trzeciego.

191 W tym względzie Komisja zaznaczyła w motywie 115 decyzji w sprawie Tarczy Prywatności, że „[c]hociaż osoby fizyczne, w tym osoby z [Unii], […] mają zatem liczne możliwości dochodzenia roszczeń, jeżeli zostały objęte bezprawnym dozorem (elektronicznym) do celów bezpieczeństwa narodowego, równie oczywiste jest, że nie uwzględniono przynajmniej niektórych podstaw prawnych, na jakie mogą powołać się amerykańskie organy wywiadowcze (np. rozporządzenie wykonawcze nr 12333)”. W zakresie dotyczącym rozporządzenia wykonawczego nr 12333 w motywie tym instytucja ta położyła nacisk w szczególności na brak jakichkolwiek środków zaskarżenia. Zgodnie zaś z orzecznictwem przypomnianym w pkt 187 niniejszego wyroku tego rodzaju luka w ochronie sądowej przed ingerencjami związanymi z programami nadzoru opartymi na tym dekrecie prezydenckim stoi na przeszkodzie temu, by uznać, jak uczyniła to Komisja w decyzji w sprawie Tarczy Prywatności, że prawo Stanów Zjednoczonych zapewnia stopień ochrony merytorycznie równoważny temu gwarantowanemu w art. 47 karty.

192 Ponadto, co się tyczy zarówno programów nadzoru opartych na art. 702 FISA, jak i tych opartych na rozporządzeniu wykonawczym nr 12333, w pkt 181 i 182 niniejszego wyroku wskazano, że ani w PPD-28, ani w rozporządzeniu wykonawczym nr 12333 nie przyznano osobom, których dane są przetwarzane, praw, które mogłyby być egzekwowalne przed sądami, wobec czego osoby te nie mają prawa do skutecznego środka prawnego.

193 Komisja stwierdziła jednak w motywach 115 i 116 decyzji w sprawie Tarczy Prywatności, że, ze względu na utworzenie przez organy władz amerykańskich urzędu Rzecznika, który został opisany w znajdującym się w załączniku III do tej decyzji piśmie sekretarza stanu USA skierowanego w dniu 7 lipca 2016 r. do unijnego komisarza ds. sprawiedliwości, konsumentów i równouprawnienia płci, oraz charakter powierzonego temu Rzecznikowi zadania, w niniejszym przypadku „starszego koordynatora ds. międzynarodowej dyplomacji w dziedzinie technologii informacyjnej”, można uznać, że zapewniany przez Stany Zjednoczone stopień ochrony jest merytorycznie równoznaczny z tym zagwarantowanym w art. 47 karty.

194 Przy badaniu kwestii, czy ten fakt istnienia urzędu Rzecznika, o którym mowa w decyzji w sprawie Tarczy Prywatności, rzeczywiście może zaradzić stwierdzonym przez Komisję ograniczeniom prawa do ochrony sądowej, należy zgodnie z wymogami ustanowionymi w art. 47 karty i w orzecznictwie przypomnianym w pkt 187 niniejszego wyroku wyjść z założenia, że jednostkom powinna przysługiwać możliwość skorzystania przed niezawisłym i bezstronnym sądem ze środków prawnych w celu uzyskania dostępu do dotyczących ich danych osobowych lub spowodowania korekty lub usunięcia takich danych.

195 Tymczasem w piśmie, o którym mowa w pkt 193 niniejszego wyroku, Rzecznik ds. Tarczy Prywatności, choć opisany jako „niezależny od Wspólnoty Wywiadowczej”, został przedstawiony jako „[podlegający] bezpośrednio sekretarzowi stanu, który zapewni, by wykonywał on zadania w sposób obiektywny i nie ulegał niepożądanym wpływom, które mogłyby wywrzeć skutek na odpowiedź, której należy udzielić”. Ponadto, poza tym, że – jak stwierdziła Komisja w motywie 116 tej decyzji – Rzecznik ten jest wyznaczany przez sekretarza stanu i stanowi integralną część departamentu stanu Stanów Zjednoczonych, w decyzji tej nie ma, jak zauważył Rzecznik generalny w pkt 337 opinii, niczego, co by świadczyło o tym, że odwołaniu Rzecznika lub unieważnieniu jego powołania towarzyszą szczególne gwarancje, co może podważać niezależność Rzecznika w stosunku do władzy wykonawczej (zob. podobnie wyrok z dnia 21 stycznia 2020 r., Banco de Santander, C-274/14, EU:C:2020:17, pkt 60, 63 i przytoczone tam orzecznictwo).

196 Podobnie, jak podkreślił Rzecznik generalny w pkt 338 opinii, choć w motywie 120 decyzji w sprawie Tarczy Prywatności mowa jest o zobowiązaniu rządu amerykańskiego do doprowadzenia do tego, by dana jednostka służb wywiadowczych podjęła działania naprawcze w związku z wszelkimi wykrytymi przez Rzecznika ds. Tarczy Prywatności naruszeniami obowiązujących przepisów, to jednak ta decyzja nie zawiera żadnego elementu świadczącego o tym, że jest on uprawniony do podejmowania decyzji wiążących te służby, ani też nie wskazuje na istnienie gwarancji prawnych, z którymi wiązałoby się to zobowiązanie i na które mogłyby się powołać osoby, których dane dotyczą.

197 W związku z tym fakt istnienia Rzecznika ds. Tarczy Prywatności, o którym mowa w decyzji w sprawie Tarczy Prywatności, nie daje możliwości podniesienia środka odwoławczego przed organem oferującego osobom, których dane są przekazywane do Stanów Zjednoczonych, zabezpieczenia merytorycznie równoważne tym wymaganym w art. 47 karty.

198 Tak więc, stwierdzając w art. 1 ust. 1 decyzji w sprawie Tarczy Prywatności, że Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii podmiotom mającym siedzibę w tym państwie trzecim w ramach Tarczy Prywatności Unia Europejska–USA, Komisja naruszyła wymogi wynikające z art. 45 ust. 1 RODO w związku z art. 7, 8 i 47 karty.

199 Z powyższego wynika, że art. 1 decyzji w sprawie Tarczy Prywatności jest niezgodny z art. 45 ust. 1 RODO w związku z art. 7, 8 i 47 karty i z tego względu nieważny.

200 Skoro zaś art. 1 decyzji w sprawie Tarczy Prywatności jest nierozerwalnie związany z jej art. 2–6, a także z załącznikami do tej decyzji, nieważność art. 1 ma wpływ na ważność tej decyzji w całości.

201 W świetle wszystkich powyższych rozważań należy uznać, że decyzja w sprawie Tarczy Prywatności jest nieważna.

202 Co się tyczy kwestii, czy należy utrzymać w mocy skutki tej decyzji w celu uniknięcia powstania luki prawnej (zob. podobnie wyrok z dnia 28 kwietnia 2016 r., Borealis Polyolefine i in., C-191/14, C-192/14, C-295/14, C-389/14 i od C-391/14 do C-393/14, EU:C:2016:311, pkt 106), należy zauważyć, że w każdym razie, biorąc pod uwagę art. 49 RODO, stwierdzenie nieważności decyzji o odpowiednim stopniu ochrony, takiej jak decyzja w sprawie Tarczy Prywatności, nie może spowodować powstania takiej luki prawnej. W artykule tym określono bowiem w sposób precyzyjny warunki, na jakich może nastąpić przekazywanie danych osobowych do państw trzecich w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony na zasadach przewidzianych art. 45 ust. 3 tego rozporządzenia lub właściwych zabezpieczeń na zasadach przewidzianych w art. 46 tego rozporządzenia.

W przedmiocie kosztów

203 Dla stron w postępowaniu głównym niniejsze postępowanie ma charakter incydentalny, dotyczy bowiem kwestii podniesionej przed sądem odsyłającym, do niego zatem należy rozstrzygnięcie o kosztach. Koszty poniesione w związku z przedstawieniem uwag Trybunałowi, inne niż koszty stron w postępowaniu głównym, nie podlegają zwrotowi.

Z powyższych względów Trybunał (wielka izba) orzeka, co następuje:

1) **Artykuł 2 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych) należy interpretować w ten sposób, że zakresem stosowania tego rozporządzenia jest objęte przekazywanie danych osobowych przez podmiot gospodarczy mający siedzibę w jednym państwie członkowskim innemu**

podmiotowi gospodarczemu z siedzibą w państwie trzecim, niezależnie od faktu, że w trakcie tego przekazywania lub w jego następstwie dane te mogą być przetwarzane przez organy władzy danego państwa trzeciego w celach związanych z bezpieczeństwem publicznym, obronnością i bezpieczeństwem państwa.

2) **Artykuł 46 ust. 1 i art. 46 ust. 2 lit. c) rozporządzenia 2016/679 należy interpretować w ten sposób, że wymagane przez te przepisy odpowiednie zabezpieczenia, egzekwowalne prawa oraz skuteczne środki ochrony prawnej powinny zapewniać, by prawa osób, których dane osobowe są przekazywane do państwa trzeciego na podstawie standardowych klauzul ochrony danych, były chronione w stopniu merytorycznie równoważnym temu gwarantowanemu w Unii przez to rozporządzenie, interpretowane w świetle Karty praw podstawowych Unii Europejskiej. W tym celu w ramach oceny stopnia ochrony zapewnianego w kontekście takiego przekazywania należy w szczególności uwzględniać zarówno postanowienia umowne uzgodnione między mającymi siedzibę w Unii administratorem lub podmiotem przetwarzającym a odbierającym dane podmiotem mającym siedzibę w danym państwie trzecim, jak i, w odniesieniu do ewentualnego dostępu organów władzy publicznej tego państwa trzeciego do przekazanych w ten sposób danych osobowych, istotne elementy składające się na jego system prawny, w szczególności te wymienione w art. 45 ust. 2 wspomnianego rozporządzenia.**

3) **Artykuł 58 ust. 2 lit. f) i j) rozporządzenia 2016/679 należy interpretować w ten sposób, że – o ile nie istnieje ważna decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony danych – właściwy organ nadzorczy jest zobowiązany do zawieszenia lub zakazania przekazywania danych do państwa trzeciego na podstawie standardowych klauzul ochrony danych przyjętych przez Komisję, jeżeli ten organ nadzorczy w świetle całokształtu okoliczności towarzyszących temu przekazywaniu uzna, że klauzule te nie są lub nie mogą być przestrzegane w tym państwie trzecim, a ochrona przekazywanych danych, jakiej wymaga prawo unijne, a w szczególności art. 45 i 46 tego rozporządzenia i Karta praw podstawowych Unii Europejskiej, nie może być zapewniona za pomocą innych środków, jeśli to przekazywanie danych nie zostało zawieszone lub zakończone przez samych mających siedzibę w Unii administratora lub podmiot przetwarzający.**

4) **Przeprowadzone w świetle art. 7, 8 i 47 Karty praw podstawowych badanie decyzji Komisji 2010/87/UE z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podwykonawcom mającym siedzibę w państwach trzecich na podstawie dyrektywy Parlamentu Europejskiego i Rady 95/46/WE, zmienionej decyzją wykonawczą Komisji (UE) 2016/2297 z dnia 16 grudnia 2016 r., nie doprowadziło do żadnych ustaleń, które mogłyby mieć wpływ na ważność tej decyzji.**

5) **Decyzja wykonawcza Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r., przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA jest nieważna.**

Podpisy