



DECYZJA WYKONAWCZA KOMISJI (UE) 2025/2571

z dnia 19 grudnia 2025 r.

zmieniająca decyzję wykonawczą Komisji (UE) 2021/1773 na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680, stwierdzającą odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo

(notyfikowana jako dokument nr C(2025) 8782)

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłającą decyzję ramową Rady 2008/977/WSiSW⁽¹⁾, w szczególności jej art. 36 ust. 3,

a także mając na uwadze, co następuje:

1. WPROWADZENIE

- (1) W decyzji wykonawczej Komisji (UE) 2021/1773⁽²⁾ stwierdzono, że do celów art. 36 dyrektywy (UE) 2016/680 Zjednoczone Królestwo zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych z Unii Europejskiej do Zjednoczonego Królestwa w zakresie stosowania tej dyrektywy.
- (2) Podczas przyjmowania decyzji wykonawczej (UE) 2021/1773 Komisja wzięła pod uwagę fakt, że wraz z zakończeniem okresu przejściowego przewidzianego w umowie o wystąpieniu Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej z Unii Europejskiej i Europejskiej Wspólnoty Energii Atomowej⁽³⁾ oraz z chwilą, gdy przestanie obowiązywać przepis przejściowy określony w art. 782 Umowy o handlu i współpracy między Unią Europejską i Europejską Wspólnotą Energii Atomowej, z jednej strony, a Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej, z drugiej strony⁽⁴⁾, Zjednoczone Królestwo może przyjąć i stosować nowy system ochrony danych, różniący się od systemu, który obowiązywał, gdy Zjednoczone Królestwo było związane prawem Unii, i egzekwować jego stosowanie.
- (3) Jako że mogłoby to wiązać się z poprawkami do ram ochrony danych poddanych ocenie w decyzji wykonawczej (UE) 2021/1773 lub innymi istotnymi zmianami, uznano za właściwe zapewnić, aby decyzja ta była stosowana przez okres czterech lat od chwili jej wejścia w życie. Decyzja wykonawcza (UE) 2021/1773 miała zatem stracić moc w dniu 27 czerwca 2025 r., chyba że zostałaby przedłużona zgodnie z procedurą, o której mowa w art. 58 ust. 2 dyrektywy (UE) 2016/680.
- (4) Aby podjąć decyzję o ewentualnym przedłużeniu obowiązywania decyzji wykonawczej (UE) 2021/1773, Komisja musi ocenić, czy wniosek, że Zjednoczone Królestwo zapewnia odpowiedni stopień ochrony, pozostaje uzasadniony pod względem faktycznym i prawnym w świetle zmian, jakie miały miejsce od czasu przyjęcia decyzji wykonawczej (UE) 2021/1773 w odniesieniu do elementów wymienionych w art. 36 ust. 2 dyrektywy (UE) 2016/680.
- (5) W dniu 23 października 2024 r. rząd Zjednoczonego Królestwa przedstawił w parlamencie Zjednoczonego Królestwa projekt ustawy o wykorzystaniu danych i dostępie do danych⁽⁵⁾, zawierający propozycje zmian w ustawie o ochronie danych z 2018 r. (DPA 2018), którą oceniono w decyzji wykonawczej (UE) 2021/1773.

⁽¹⁾ Dz.U. L 119 z 4.5.2016, s. 89, ELI: <http://data.europa.eu/eli/dir/2016/680/oj>.

⁽²⁾ Decyzja wykonawcza Komisji (UE) 2021/1773 z dnia 28 czerwca 2021 r. na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680, stwierdzająca odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo (Dz.U. L 360 z 11.10.2021, s. 69, ELI: http://data.europa.eu/eli/dec_impl/2021/1773/oj).

⁽³⁾ Dz.U. C 384 I z 12.11.2019, s. 1.

⁽⁴⁾ Dz.U. L 149 z 30.4.2021, s. 10, ELI: [http://data.europa.eu/eli/agree_internation/2021/689\(1\)/oj](http://data.europa.eu/eli/agree_internation/2021/689(1)/oj).

⁽⁵⁾ Dostęp pod adresem: <https://bills.parliament.uk/bills/3825/news>.

W dniu 24 czerwca 2025 r. Komisja przyjęła decyzję wykonawczą Komisji (UE) 2025/1225 ⁽⁶⁾, która przedłużyła obowiązywanie decyzji (UE) 2021/1773 o sześć miesięcy, do dnia 27 grudnia 2025 r. To ograniczone w czasie przedłużenie techniczne umożliwiło Komisji sfinalizowanie oceny, czy Zjednoczone Królestwo zapewnia odpowiedni stopień ochrony danych osobowych, na podstawie stabilnych ram prawnych, tj. po zakończeniu odpowiedniego procesu legislacyjnego.

- (6) Od czasu przyjęcia decyzji wykonawczej (UE) 2021/1773 Komisja na bieżąco monitorowała istotne zmiany w Zjednoczonym Królestwie ⁽⁷⁾. Zgodnie z motywem 165 decyzji wykonawczej 2021/1773 szczególną uwagę zwrócono na stosowanie w praktyce przepisów Zjednoczonego Królestwa dotyczących przekazywania danych osobowych do państw trzecich oraz na wpływ, jaki może to mieć na stopień ochrony zapewnianej danym przekazywanym na mocy decyzji wykonawczej (UE) 2021/1773, oraz na skuteczność wykonywania praw indywidualnych, w tym na wszelkie istotne zmiany w prawie i praktyce dotyczące wyjątków lub ograniczeń takich praw. W monitorowaniu Komisja uwzględniła między innymi zmiany w orzecznictwie oraz nadzór ze strony Komisarza ds. Informacji i innych niezależnych organów.
- (7) Na podstawie oceny tych zmian, w tym zmian w DPA 2018 wprowadzonych ustawą o wykorzystaniu danych i dostępie do danych, Komisja stwierdza, że Zjednoczone Królestwo nadal zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych w ramach zakresu dyrektywy (UE) 2016/680 z Unii Europejskiej do Zjednoczonego Królestwa.

2. ISTOTNE ZMIANY DOTYCZĄCE PRZEPISÓW MAJĄCYCH ZASTOSOWANIE DO PRZETWARZANIA DANYCH OSOBOWYCH

2.1. Ramy ochrony danych obowiązujące w Zjednoczonym Królestwie

- (8) W momencie przyjęcia decyzji wykonawczej (UE) 2021/1773 ramy prawne przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom w Zjednoczonym Królestwie, określono w odpowiednich częściach DPA 2018 ⁽⁸⁾, zmienionej rozporządzeniem w sprawie ochrony danych, prywatności i łączności elektronicznej wprowadzającym zmiany w związku z wyjściem z UE z 2019 r. (rozporządzenie DPPEC) ⁽⁹⁾, w szczególności w części 3 tej ustawy.
- (9) Chociaż ustawa ta, która ściśle odzwierciedlała odpowiednie przepisy mające zastosowanie w Unii Europejskiej, nadal stanowi prawodawstwo Zjednoczonego Królestwa w zakresie ochrony danych w odniesieniu do stosownych czynności przetwarzania, od tego czasu podlegała pewnym ograniczonym zmianom, co odzwierciedla fakt, że Zjednoczone Królestwo nie podlega już prawu Unii Europejskiej.
- (10) Po pierwsze, w ustawie o zachowanym prawie UE (i uchyleniu lub reformie niektórych przepisów) z 2023 r. (ustawa REUL) ⁽¹⁰⁾ wyjaśniono, że od końca 2023 r. ogólne zasady prawa UE nie są już częścią prawa krajowego Zjednoczonego Królestwa ⁽¹¹⁾. Ponadto sądy Zjednoczonego Królestwa nie muszą już dokonywać wykładni

⁽⁶⁾ Decyzja wykonawcza Komisji (UE) 2025/1225 z dnia 24 czerwca 2025 r. zmieniająca decyzję wykonawczą (UE) 2021/1773 na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680, stwierdzającą odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo (Dz.U. L, 2025/1225, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1225/oj).

⁽⁷⁾ Art. 36 ust. 4 dyrektywy (UE) 2016/680.

⁽⁸⁾ Ustawa o ochronie danych z 2018 r., dostępna pod adresem: <https://www.legislation.gov.uk/ukpga/2018/12/contents>. Przed wystąpieniem Zjednoczonego Królestwa z Unii Europejskiej i w okresie przejściowym DPA 2018 przewidywała, w przypadkach dozwolonych na mocy rozporządzenia (UE) 2016/679, przepisy krajowe określające i ograniczające stosowanie przepisów rozporządzenia (UE) 2016/679 i transponowanej dyrektywy (UE) 2016/680.

⁽⁹⁾ Rozporządzenie w sprawie ochrony danych, prywatności i łączności elektronicznej wprowadzające zmiany w związku z wyjściem z UE z 2019 r., dostępne pod adresem: <https://www.legislation.gov.uk/uksi/2019/419/contents/made>, zmienione rozporządzeniem DPPEC z 2020 r., dostępnym pod adresem: <https://www.legislation.gov.uk/ukdsi/2020/9780348213522>. Rozporządzenie DPPEC zmienia rozporządzenie (UE) 2016/679 wprowadzone do prawa Zjednoczonego Królestwa w drodze ustawy o wystąpieniu z Unii Europejskiej z 2018 r., DPA 2018 i innych przepisów o ochronie danych, aby dostosować te przepisy do kontekstu krajowego.

⁽¹⁰⁾ Ustawa o zachowanym prawie UE (i uchyleniu lub reformie niektórych przepisów) z 2023 r., dostępna pod adresem: <https://www.legislation.gov.uk/ukpga/2023/28>.

⁽¹¹⁾ Art. 5 ustawy o wystąpieniu z Unii Europejskiej z 2018 r., zmienionej ustawą REUL.

niezmienionego „prawa asymilowanego” – które wcześniej określano jako „zachowane prawo UE” – zgodnie z ogólnymi zasadami prawa UE, ale prawo takie musi być odczytywane w sposób zgodny z prawem krajowym Zjednoczonego Królestwa⁽¹²⁾. Odpowiednie sądy Zjednoczonego Królestwa muszą jednak nadal dokonywać wykładni niezmiennego prawa asymilowanego zgodnie ze stosownym orzecznictwem Europejskiego Trybunału Sprawiedliwości wydanym przed zakończeniem okresu przejściowego⁽¹³⁾, jak wspomniano również w motywie 12 decyzji wykonawczej (UE) 2021/1773. DPA 2018 została zmieniona ustawą o wykorzystaniu danych i dostępie do danych w celu wyjaśnienia wpływu ustawy REUL na przepisy Zjednoczonego Królestwa o ochronie danych. Na przykład art. 183 A ust. 1 DPA 2018 stanowi, że co do zasady wszelkie nowe przepisy (przyjęte w dniu 20 sierpnia 2025 r. lub po tej dacie), które wprowadzają nowe obowiązki lub uprawnienia w zakresie przetwarzania danych osobowych, uznaje się za podlegające przepisom Zjednoczonego Królestwa o ochronie danych. Oznacza to, że brytyjskie ramy ochrony danych nadal mają pierwszeństwo przed innymi przepisami. Zgodnie z art. 183 A ust. 2 lit. b) DPA 2018 odstąpienie od stosowania tego domniemania jest możliwe, jeżeli parlament Zjednoczonego Królestwa wyraźnie postanowi o tym w ustawodawstwie, zachowując suwerenność parlamentarną. Ponadto w art. 186 ust. 2 A DPA 2018 wyjaśniono, że ograniczenia praw osób, których dane dotyczą, wymienione w art. 186 ust. 3 DPA 2018 nie podlegają zasadzie zawartej w art. 186 ust. 1 DPA 2018, który stanowi, że przepisy zakazujące ujawniania informacji lub ograniczające ujawnianie informacji nie są nadrzędne wobec niektórych praw do ochrony danych. Gwarantuje to na przykład, że ograniczenia praw osób, których dane dotyczą, określone w DPA 2018, same w sobie nie są objęte ogólną zasadą nadrzędności ochrony danych określoną w art. 186 ust. 1 DPA 2018.

- (11) Po drugie, od czasu przyjęcia decyzji wykonawczej (UE) 2021/1773 przepisy Zjednoczonego Królestwa o ochronie danych zostały już zmienione rozporządzeniem zmieniającym w sprawie podstawowych praw i wolności w zakresie ochrony danych z 2023 r.⁽¹⁴⁾ W rozporządzeniu tym zdefiniowano odniesienia do praw podstawowych lub podstawowych wolności w DPA 2018 (które wcześniej zdefiniowano tak, aby obejmowały prawa podstawowe i podstawowe wolności UE⁽¹⁵⁾) jako odniesienia do praw wynikających z europejskiej konwencji praw człowieka, które stały się skuteczne w prawie krajowym Zjednoczonego Królestwa na mocy ustawy o prawach człowieka z 1998 r.⁽¹⁶⁾ Ustawą o prawach człowieka z 1998 r. wprowadzono do prawa Zjednoczonego Królestwa prawa zawarte w europejskiej konwencji praw człowieka. Ustawa o prawach człowieka zapewnia każdej osobie fizycznej podstawowe prawa i wolności przewidziane w art. 2–12 i 14 europejskiej konwencji praw człowieka, art. 1, 2 i 3 pierwszego protokołu do niej oraz art. 1 trzynastego protokołu do niej w związku z art. 16, 17 i 18 tej konwencji. Należą do nich prawo do poszanowania życia prywatnego i rodzinnego (i prawo do ochrony danych osobowych jako element tego prawa) oraz prawo do rzetelnego procesu sądowego⁽¹⁷⁾.
- (12) Ponadto DPA 2018 była przedmiotem ukierunkowanych reform przewidzianych w częściach piątej i szóstej ustawy o wykorzystaniu danych i dostępie do danych. Chociaż zakres ustawy o wykorzystaniu danych i dostępie do danych znacznie wykracza poza ochronę danych osobowych, ustawa przewiduje ograniczone zmiany w kilku aspektach systemu ochrony danych, takich jak m.in. warunki wykonywania praw osób, których dane dotyczą, warunki zautomatyzowanego podejmowania decyzji oraz zakres niektórych wymogów dotyczących rozliczalności. Ponadto ustawą o wykorzystaniu danych i dostępie do danych wprowadzono zmiany w strukturze zarządzania podmiotu, jakim jest Komisarz ds. Informacji. Po wdrożeniu tych zmian Komisarza ds. Informacji zastąpi nowy podmiot – Komisja ds. Informacji. Rola i funkcje organu regulacyjnego jako niezależnego organu nadzorczego ds. ochrony danych w Zjednoczonym Królestwie pozostaną niezmienione. Ustawa wprowadza również nowe uprawnienia wykonawcze organu regulacyjnego.
- (13) W niniejszej decyzji oceniono zmiany ustawodawcze, regulacyjne i inne, które są istotne dla wniosku dotyczącego stopnia ochrony gwarantowanego przez Zjednoczone Królestwo zawartego w decyzji wykonawczej (UE) 2021/1773. Ocena przeprowadzona w decyzji wykonawczej (UE) 2021/1773 pozostaje ważna w odniesieniu do aspektów ram ochrony danych Zjednoczonego Królestwa, które nie podlegały zmianom lub na które nie miały wpływu inne zmiany od czasu przyjęcia decyzji wykonawczej (UE) 2021/1773.

⁽¹²⁾ Art. 5 ust. A2 ustawy o wystąpieniu z Unii Europejskiej z 2018 r., zmienionej ustawą REUL.

⁽¹³⁾ Art. 6 ust. 3 i 7 ustawy o wystąpieniu z Unii Europejskiej z 2018 r., zmienionej ustawą REUL.

⁽¹⁴⁾ Dostęp pod adresem: <https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023>.

⁽¹⁵⁾ Prawa podstawowe i podstawowe wolności UE zachowano w prawie Zjednoczonego Królestwa na mocy art. 4 ustawy o wystąpieniu z Unii Europejskiej z 2018 r., który uchylono pod koniec 2023 r. ustawą REUL.

⁽¹⁶⁾ Art. 2 ust. 3 rozporządzenia zmieniającego w sprawie podstawowych praw i wolności w zakresie ochrony danych z 2023 r.

⁽¹⁷⁾ Art. 6, 8, 10 i 13 EKPC (zob. także załącznik 1 do ustawy o prawach człowieka z 1998 r., dostępny pod adresem: <https://www.legislation.gov.uk/ukpga/1998/42/contents>).

- (14) Zmiany ustawodawcze, regulacyjne i inne istotne zmiany szczegółowo przeanalizowano w kolejnych sekcjach na podstawie odpowiedniego standardu ochrony, zgodnie z którym Komisja musi ustalić, czy dane państwo trzecie gwarantuje stopień ochrony „merytorycznie równoważny” stopniowi ochrony zapewnianemu w Unii Europejskiej ⁽¹⁸⁾. Jak wyjaśnił w swoim orzecznictwie Trybunał Sprawiedliwości Unii Europejskiej, nie oznacza to konieczności stwierdzenia identycznego stopnia ochrony ⁽¹⁹⁾. W szczególności środki, z jakich korzysta dane państwo trzecie do zapewnienia ochrony danych osobowych, mogą różnić się od środków wprowadzonych w Unii Europejskiej, o ile w praktyce skutecznie zapewniają odpowiedni stopień ochrony ⁽²⁰⁾. Odpowiedni standard ochrony nie wymaga zatem dokładnego powielenia przepisów unijnych. W badaniu, czy stopień ochrony jest odpowiedni, chodzi raczej o stwierdzenie, czy biorąc pod uwagę istotę prawa do ochrony danych oraz jego skuteczne wprowadzenie w życie, egzekwowanie i nadzór nad jego przestrzeganiem, konkretny zagraniczny system prawny zapewnia jako całość wymagany stopień ochrony ⁽²¹⁾.

2.1.1. Definicje

- (15) Podstawowe pojęcia z dziedziny ochrony danych odzwierciedlające terminologię dyrektywy (UE) 2016/680 nadal mają zastosowanie w systemie ochrony danych Zjednoczonego Królestwa. Pojęcia te oceniono w motywach 26 i 27 decyzji wykonawczej (UE) 2021/1773.
- (16) W szczególności – poprzez określenie definicji i warunków uzyskania zgody – w ustawie o wykorzystaniu danych i dostępie do danych potwierdzono ramy prawne regulujące wykorzystywanie zgody jako przewidzianej w prawie podstawy przetwarzania danych osobowych ⁽²²⁾. Zaktualizowane przepisy powielają brzmienie RODO UK, zwiększając tym samym spójność między systemami ochrony danych Zjednoczonego Królestwa. To uspołnienie przyczynia się do jaśniejszej interpretacji przez właściwe organy w przypadkach, gdy podstawą prawną przetwarzania przez nie danych osobowych jest zgoda.
- (17) Po pierwsze, art. 69 ustawy o wykorzystaniu danych i dostępie do danych wprowadza do DPA 2018 nowy art. 33 ust. 1 A, w którym zdefiniowano „zgoda” jako dobrowolne, konkretne, świadome i jednoznaczne okazanie woli osoby, której dane dotyczą. Takie okazanie woli musi mieć formę oświadczenia lub wyraźnego działania potwierdzającego i musi oznaczać przyzwolenie danej osoby na przetwarzanie jej danych osobowych.
- (18) Po drugie, tym samym artykułem dodano do DPA 2018 art. 40 A, określający warunki, które należy spełnić w przypadku opierania się na zgodzie. Administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła ważną zgodę. W przypadku gdy zgodę uzyskuje się na piśmie jako część szerszego dokumentu, musi być ona wyrażona w sposób wyraźnie odróżniający ją od innych kwestii, przy użyciu dostępnego, zrozumiałego i prostego języka. Postanowienia takiego dokumentu, które nie są zgodne z tymi standardami, nie są wiążące ⁽²³⁾.
- (19) Administratorzy lub podmioty przetwarzające muszą również poinformować daną osobę fizyczną przed uzyskaniem zgody o przysługującym jej prawie do wycofania zgody. Procedura wycofania musi być równie łatwa jak procedura udzielania zgody. Dzięki temu osoba, której dane dotyczą, zachowuje rzeczywistą kontrolę nad wykorzystywaniem swoich danych osobowych przez cały czas ⁽²⁴⁾.
- (20) Ponadto w ustawie o wykorzystaniu danych i dostępie do danych wyjaśniono, że przy ocenie, czy zgoda jest udzielana „dobrowolnie”, należy rozważyć, czy świadczenie usługi było uzależnione od wyrażenia przez osobę, której dane dotyczą, zgody na przetwarzanie danych osobowych, które nie jest wymagane do świadczenia tej usługi. W takim przypadku może to podważyć ważność zgody ⁽²⁵⁾.

⁽¹⁸⁾ Motyw 67 dyrektywy (UE) 2016/680.

⁽¹⁹⁾ Sprawa C-362/14, Schrems („Schrems I”), ECLI:EU:C:2015:650, pkt 73.

⁽²⁰⁾ Schrems I, pkt 74.

⁽²¹⁾ Zob. komunikat Komisji do Parlamentu Europejskiego i Rady „Wymiana i ochrona danych osobowych w zglobalizowanym świecie”, COM(2017) 7 z dnia 10 stycznia 2017 r., pkt 3.1, s. 7, dostępny pod adresem: <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52017DC0007>.

⁽²²⁾ Art. 33 i 40 A DPA 2018, wprowadzone art. 69 ust. 1, 2 i 4 ustawy o wykorzystaniu danych i dostępie do danych.

⁽²³⁾ Art. 40 A ust. 2 i 3 DPA 2018, wprowadzone art. 69 ust. 4 ustawy o wykorzystaniu danych i dostępie do danych.

⁽²⁴⁾ Art. 40 A ust. 5 i 6 DPA 2018, wprowadzone art. 69 ust. 4 ustawy o wykorzystaniu danych i dostępie do danych.

⁽²⁵⁾ Art. 40 A ust. 7 DPA 2018, wprowadzony art. 69 ust. 4 ustawy o wykorzystaniu danych i dostępie do danych.

- (21) Co ważne, zgodnie ze zmienioną częścią 3 DPA 2018 zgoda nadal nie stanowi istotnej podstawy prawnej w odniesieniu do operacji przetwarzania wchodzących w zakres stosowania niniejszej decyzji, jak wyjaśniono w motywie 35 decyzji wykonawczej (UE) 2021/1773. Ponadto, jak zauważono w motywie 36 decyzji wykonawczej (UE) 2021/1773, przetwarzanie w kontekście ścigania przestępstw nadal nie jest możliwe wyłącznie na podstawie zgody, ponieważ właściwy organ musi zawsze posiadać odpowiednie uprawnienia, które umożliwiają mu przetwarzanie danych. Mówiąc ściślej, oznacza to – podobnie do tego, co dopuszcza dyrektywa (UE) 2016/680⁽²⁶⁾ – że zgoda służy jako dodatkowy warunek umożliwiający przeprowadzenie niektórych ograniczonych i szczególnych operacji przetwarzania, które w inny sposób nie mogłyby zostać przeprowadzone, na przykład pobranie i przetwarzanie próbki DNA osoby fizycznej niebędącej podejrzanym.

2.2. Zabezpieczenia, prawa i obowiązki

2.2.1. Przetwarzanie wrażliwych danych osobowych

- (22) Ramy ochrony danych Zjednoczonego Królestwa nadal zapewniają szczególne zabezpieczenia w przypadku szczególnych kategorii danych, jak oceniono w motywach 38–42 decyzji wykonawczej (UE) 2021/1773.
- (23) Zarówno definicja szczególnych kategorii danych osobowych, jak i szczegółowe przepisy mające zastosowanie do przetwarzania tych kategorii danych w części 3 DPA 2018 pozostają w mocy. Jednocześnie ustawa o wykorzystaniu danych i dostępie do danych przyznaje Sekretarzowi Stanu nowe uprawnienia w zakresie wydawania rozporządzeń dodających nowe szczególne kategorie danych i dostosowujących, w razie potrzeby, warunki ich wykorzystywania⁽²⁷⁾. Co ważne, uprawnienie to nie pozwala Sekretarzowi Stanu na usunięcie lub zmianę istniejących szczególnych kategorii danych ani na zmianę warunków przetwarzania tych kategorii⁽²⁸⁾.
- (24) W związku z tym zmiany te nie mają wpływu na stopień ochrony szczególnych kategorii danych osobowych uznany w decyzji wykonawczej (UE) 2021/1773 za zasadniczo odpowiadający (tzn. merytorycznie równoważny) ochronie w UE.

2.2.2. Prawa indywidualne

- (25) Zgodnie z ramami prawnymi Zjednoczonego Królestwa osoby, których dane dotyczą, nadal korzystają z tych samych praw indywidualnych co na mocy dyrektywy (UE) 2016/680, a prawa te mogą być egzekwowane wobec administratora lub podmiotu przetwarzającego, w szczególności z prawa dostępu do danych, prawa do sprzeciwu wobec przetwarzania oraz prawa do sprostowania i usunięcia danych, jak oceniono w motywach 57–65 decyzji wykonawczej (UE) 2021/1773.
- (26) W ustawie o wykorzystaniu danych i dostępie do danych wyjaśniono pewne warunki wykonywania tych praw.
- (27) Po pierwsze, w ramach obecnego systemu administratorzy danych mają prawo odrzucić żądanie lub pobrać zasadną opłatę, jeżeli żądanie jest w sposób oczywisty nieuzasadnione lub nadmiernie wygórowane⁽²⁹⁾. W tym względzie ustawa o wykorzystaniu danych i dostępie do danych przyznaje Sekretarzowi Stanu nowe uprawnienia regulacyjne, umożliwiając Sekretarzowi Stanu wydawanie rozporządzeń nakładających na administratorów danych obowiązek opracowywania i publikowania wytycznych dotyczących opłat pobieranych przez nich w takich okolicznościach. Ponadto w ustawie o wykorzystaniu danych i dostępie do danych doprecyzowano, że w przypadku gdy administrator danych odmawia uznania żądania ze wspomnianej wyżej przyczyny, jest on nadal obowiązany powiadomić osobę, której dane dotyczą, o przyczynach odmowy, oraz o przysługującym tej osobie prawie do złożenia skargi do Komisarza ds. Informacji. Takie powiadomienie należy przekazać bez zbędnej zwłoki⁽³⁰⁾.
- (28) Po drugie, w ustawie o wykorzystaniu danych i dostępie do danych określono terminy, w których administratorzy danych muszą odpowiedzieć na żądania osoby, której dane dotyczą. Dokładniej rzecz ujmując, dostosowuje ona wymagane terminy na odpowiedź do terminów określonych w RODO UK. Zmienione przepisy umożliwiają również przedłużenie terminu na odpowiedź o maksymalnie dwa dodatkowe miesiące w przypadkach, gdy żądanie

⁽²⁶⁾ Zob. motywy 35 i 37 dyrektywy (UE) 2016/680.

⁽²⁷⁾ Art. 74 ustawy o wykorzystaniu danych i dostępie do danych. Takie rozporządzenia podlegają procedurze zatwierdzającej (ang. *affirmative resolution*), co oznacza, że wymagają aktywnego zatwierdzenia przez parlament Zjednoczonego Królestwa.

⁽²⁸⁾ Zob. nowy art. 42 A DPA 2018, wprowadzony art. 74 ustawy o wykorzystaniu danych i dostępie do danych, a także noty wyjaśniające do projektu ustawy o wykorzystaniu danych i dostępie do danych, pkt 577, dostępne pod następującym adresem: <https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf>.

⁽²⁹⁾ Art. 53 ust. 1 DPA 2018. Zob. także motyw 64 decyzji wykonawczej (UE) 2021/1773.

⁽³⁰⁾ Art. 53 ust. 4 A, 6 i 7 DPA 2018, wprowadzone art. 75 ustawy o wykorzystaniu danych i dostępie do danych.

ma złożony charakter lub gdy otrzymano wiele żądań. W takich przypadkach administrator musi poinformować osobę, której dane dotyczą, o przedłużeniu terminu i jego powodach ⁽³¹⁾. Ustawą o wykorzystaniu danych i dostępie do danych wprowadzono również mechanizm, który umożliwia administratorom zawieszenie biegu terminu udzielenia odpowiedzi na żądanie w przypadkach, gdy potrzebne są dalsze informacje od osoby, której dane dotyczą, w celu zidentyfikowania żądanych danych ⁽³²⁾.

- (29) Po trzecie, w odniesieniu do wyłącznie do prawa dostępu do informacji i danych osobowych, ustawą o wykorzystaniu danych i dostępie do danych zmieniono art. 15 RODO UK, aby uwzględnić w nim doprecyzowanie, które – w oparciu o obowiązującą w prawie UE zasadę proporcjonalności – wykształciło się w dotychczasowym orzecznictwie krajowym i zgodnie z którym administratorzy są obowiązani jedynie przeprowadzać rozsądne i proporcjonalne wyszukiwanie żądanych informacji i danych osobowych ⁽³³⁾. Oczekuje się, że nowy przepis będzie interpretowany zgodnie z istniejącym orzecznictwem, które stanowi, że „w ramach analizy proporcjonalności waży się końcowy cel wyszukiwania – a mianowicie potencjalną korzyść, jaką przekazanie informacji mogłoby przynieść osobie, której dane dotyczą – oraz środki, za pomocą których uzyskuje się te informacje. W każdym konkretnym przypadku należy ocenić, czy znalezienie i dostarczenie danych informacji będzie wymagało niewspółmiernie dużego wysiłku w stosunku do korzyści, jakie mogą one przynieść osobie, której dane dotyczą” ⁽³⁴⁾.
- (30) W związku z tym, chociaż warunki udzielania odpowiedzi na żądania osób, których dane dotyczą, podlegają bardziej szczegółowym przepisom, system Zjednoczonego Królestwa nadal zapewnia, aby żądania osób, których dane dotyczą, rozpatrywano w rozsądnych terminach określonych na podstawie obiektywnych czynników. Ponadto istotne obowiązki administratora przy udzielaniu odpowiedzi na żądania udzielenia dostępu są określone na podstawie ustalonych standardów prawnych, które uwzględniają również interesy osoby, której dane dotyczą. Już obecne wytyczne Komisarza ds. Informacji zawierają wskazanie, że administrator nie jest zobowiązany do przeprowadzania wyszukiwań, które byłyby nieuzasadnione lub nieproporcjonalne do tego, jak ważne jest zapewnienie dostępu do informacji ⁽³⁵⁾.
- (31) Ponadto ustawą o wykorzystaniu danych i dostępie do danych wprowadzono do DPA 2018 nowy art. 45 A, przewidujący wyraźne wyłączenie z obowiązku zapewnienia dostępu lub udzielenia informacji osobie, której dane dotyczą, w przypadku gdy dane informacje są chronione prawniczą tajemnicą zawodową ⁽³⁶⁾. Wyłączenie to ma zastosowanie w szczególności do obowiązków wynikających z art. 44 ust. 2 i art. 45 ust. 1 DPA 2018, które wymagają od administratorów informowania osób fizycznych o przetwarzaniu ich danych osobowych i udzielania im dostępu do tych danych ⁽³⁷⁾. W nowym artykule wyjaśniono, że administratorzy nie są zobowiązani do ujawniania informacji, jeżeli naruszałoby to prawniczą tajemnicę zawodową. Podobne wyłączenie obowiązuje na mocy RODO UK ⁽³⁸⁾.
- (32) Jeżeli chodzi o zabezpieczenia, administratorzy, powołując się na to wyłączenie, muszą bez zbędnej zwłoki poinformować na piśmie osobę, której dane dotyczą, o zastosowaniu wyłączenia, wyjaśnić przyczyny jego zastosowania oraz poinformować ją o przysługującym jej prawie do wniesienia skargi do Komisji ds. Informacji lub do skorzystania ze środków ochrony prawnej ⁽³⁹⁾. Aby zapewnić rozliczalność, w art. 45 A ust. 4 DPA 2018 zobowiązano administratorów do ewidencjonowania uzasadnień swoich decyzji o zastosowaniu wyłączenia oraz do udostępniania ich ewidencji na żądanie Komisji ds. Informacji ⁽⁴⁰⁾.

⁽³¹⁾ Art. 54 ust. 3 A oraz art. 54 ust. b 3 DPA 2018, wprowadzone art. 76 ust. 6 ustawy o wykorzystaniu danych i dostępie do danych.

⁽³²⁾ Art. 54 ust. 3C i 3D DPA 2018, wprowadzone art. 76 ust. 5 i 6 ustawy o wykorzystaniu danych i dostępie do danych.

⁽³³⁾ Art. 45 ust. 2 A DPA 2018, wprowadzony art. 78 ustawy o wykorzystaniu danych i dostępie do danych.

⁽³⁴⁾ *Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74.

⁽³⁵⁾ Dostęp pod adresem: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-find-and-retrieve-the-relevant-information/>.

⁽³⁶⁾ Art. 45 A, wprowadzony art. 79 ustawy o wykorzystaniu danych i dostępie do danych. W Zjednoczonym Królestwie prawnicza tajemnica zawodowa jest podstawowym prawem chroniącym przed ujawnieniem konkretnej poufnej komunikacji między klientem a jego doradcą prawnym bez zgody klienta. Obejmuje ona dwie główne kategorie: tajemnicę doradczą, która chroni treść komunikacji prowadzonej w celu uzyskania lub świadczenia porady prawnej, oraz tajemnicę procesową, która ma zastosowanie do komunikacji prowadzonej w ramach przygotowań do postępowania sądowego lub w jego trakcie.

⁽³⁷⁾ Właściwe organy, o których mowa w części 3, powoływały się wcześniej na inne dostępne wyłączenia przewidziane w art. 44 ust. 4 (Prawo do informacji) i art. 45 ust. 4 (Prawo dostępu) DPA 2018.

⁽³⁸⁾ Pkt 19 załącznika 2 do DPA 2018.

⁽³⁹⁾ Art. 45 A ust. 2 DPA 2018, wprowadzony art. 79 ustawy o wykorzystaniu danych i dostępie do danych. Wyjątek od tego wymogu powiadomienia ma zastosowanie w przypadku, gdy samo przekazanie takiego powiadomienia naruszyłoby uprzywilejowany lub poufny charakter informacji. W takich przypadkach administrator nie jest zobowiązany do ujawniania, że skorzystano z wyłączenia, ani do przedstawienia dalszych wyjaśnień.

⁽⁴⁰⁾ Art. 45 A DPA 2018, wprowadzony art. 79 ustawy o wykorzystaniu danych i dostępie do danych.

- (33) Ponadto ustawą o wykorzystaniu danych i dostępie do danych zmieniono i skonsolidowano istniejące wyłączenia zawarte w części 3 DPA 2018, do których właściwe organy mają dostęp w celach bezpieczeństwa narodowego. Wyłączenie dotyczące bezpieczeństwa narodowego umożliwia właściwym organom odstąpienie od stosowania niektórych przepisów części 3 DPA 2018, jeżeli wyłączenie ze stosowania tych przepisów jest wymagane do celów ochrony bezpieczeństwa narodowego⁽⁴¹⁾. Skonsolidowane wyłączenie odzwierciedla wyłączenia dotyczące bezpieczeństwa narodowego przewidziane w odniesieniu do przetwarzania danych osobowych na podstawie RODO UK (przewidziane w art. 26 DPA 2018) oraz części 4 DPA 2018 (przewidziane w art. 110 DPA 2018).
- (34) Wyłączenie dotyczące bezpieczeństwa narodowego podlega takim samym ograniczeniom i zabezpieczeniom jak wyłączenia na podstawie RODO UK i części 4 DPA 2018, które przeanalizowano w motywach 64–67 i 126 decyzji wykonawczej (UE) 2021/1772. W szczególności, wyłączenie to można stosować wyłącznie, jeżeli jest to wymagane do zapewnienia bezpieczeństwa narodowego lub obronności i wyłącznie w zakresie, w jakim jest to konieczne. Nie jest to wyłączenie ogólne, wobec czego administrator musi rozpatrywać je i powoływać się na nie osobno dla każdego przypadku⁽⁴²⁾. Ponadto każde zastosowanie wyłączenia musi być zgodne ze standardami praw człowieka (opartymi na ustawie o prawach człowieka z 1998 r. i na europejskiej konwencji praw człowieka), według których w demokratycznym społeczeństwie każda ingerencja w prawo do prywatności powinna być niezbędna i proporcjonalna⁽⁴³⁾. Znajduje to również potwierdzenie w wytycznych Komisarza ds. Informacji w zakresie stosowania wyłączeń dotyczących bezpieczeństwa narodowego⁽⁴⁴⁾.

2.2.3. Ograniczenia dotyczące dalszego przekazywania danych

- (35) Stopień ochrony zapewnianej danym osobowym przekazywanym z Unii Europejskiej organom ścigania w Zjednoczonym Królestwie nadal nie jest obniżony wskutek dalszego przekazywania takich danych odbiorcom z państw trzecich. System międzynarodowego przekazywania danych osobowych ze Zjednoczonego Królestwa pozostaje bardzo zbliżony do przepisów określonych w rozdziale V dyrektywy (UE) 2016/680, jak oceniono w motywach 74–87 decyzji wykonawczej (UE) 2021/1773.
- (36) Ustawą o wykorzystaniu danych i dostępie do danych zmieniono wprowadzić rozdział 5 części 3 DPA 2018, dotyczący przekazywania danych osobowych właściwym organom w państwach trzecich, jednak zachowano podstawowy wymóg, zgodnie z którym a) przekazanie musi być niezbędne do celów ścigania przestępstw; b) przekazanie musi (i) opierać się na rozporządzeniu zatwierdzającym przekazanie (zastępującym poprzednie rozporządzenie stwierdzające odpowiedni stopień ochrony), (ii) podlegać odpowiednim zabezpieczeniom lub (iii) opierać się na szczególnych okolicznościach oraz c) odbiorcą przekazania musi być: (i) odpowiedni organ (tj. organ równoważny właściwemu organowi) państwa trzeciego, (ii) odpowiednia organizacja międzynarodowa. (iii) podmiot przetwarzający w imieniu właściwego organu lub (iv) osoba inna niż odpowiedni organ, ale wyłącznie wówczas, gdy przekazanie jest ściśle niezbędne do realizacji jednego z celów ścigania przestępstw⁽⁴⁵⁾. Te ogólne zasady przekazywania danych znajdują odzwierciedlenie w art. 73 DPA 2018, w którym określono również, że przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej jest dozwolone tylko wtedy, gdy przekazanie odbywa się zgodnie z innymi przepisami części 3 DPA 2018⁽⁴⁶⁾.
- (37) W odniesieniu do konkretnie do rozporządzeń zatwierdzających przekazanie danych art. 74AA ust. 2 DPA 2018 stanowi, że Sekretarz Stanu może wydawać takie rozporządzenia tylko wtedy, gdy uzna, że warunki testu ochrony danych zostały spełnione. Oznacza to, że wprowadzona w art. 74AA ust. 3 DPA 2018 możliwość, aby przy wydawaniu takich rozporządzeń Sekretarz Stanu uwzględniał potrzebę ułatwienia przepływu danych, jest zawsze uzależniona od spełnienia warunków testu ochrony danych. W nowym art. 74AB⁽⁴⁷⁾ DPA 2018 sformułowano standard prawny dla spełnienia warunków testu ochrony danych, zgodnie z którym standard ochrony osób, których dane dotyczą, w państwach lub organizacjach międzynarodowych otrzymujących dane nie może być znacznie niższy niż standard zapewniany na mocy odpowiednich przepisów Zjednoczonego Królestwa o ochronie danych. Następnie

⁽⁴¹⁾ Art. 78 A ust. 1 DPA 2018, wprowadzony art. 88 ustawy o wykorzystaniu danych i dostępie do danych. Zgodnie z art. 78 A ust. 2–4 DPA 2018 wyłączenie to umożliwia odstąpienie od stosowania zasad ochrony danych (z wyjątkiem zasady zgodności z prawem oraz warunków i zabezpieczeń dotyczących przetwarzania danych wrażliwych), praw indywidualnych, obowiązków administratorów danych i podmiotów przetwarzających w odniesieniu do naruszeń ochrony danych, niektórych części regulacji dotyczących międzynarodowego przekazywania danych oraz niektórych uprawnień Komisarza ds. Informacji do wejścia do pomieszczeń w celu przeprowadzenia inspekcji i podjęcia działań w zakresie egzekwowania prawa.

⁽⁴²⁾ Zob. *Baker v Secretary of State for the Home Department* [2001] UKIT NSA2.

⁽⁴³⁾ Zob. również *Guriev v Community Safety Development (United Kingdom) Ltd*, [2016] EWHC 643 (QB), pkt 45; *Lin v Commissioner of the Police for the Metropolis* [2015] EWHC 2484 (QB), pkt 80.

⁽⁴⁴⁾ Zob. wytyczne Komisarza ds. Informacji na temat wyjątku dotyczącego bezpieczeństwa narodowego i obrony, dostępne pod adresem: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/>.

⁽⁴⁵⁾ Art. 73 DPA 2018, zmieniony przez pkt 3 ppkt 4 i 5 załącznika 8 do ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁴⁶⁾ Art. 73 DPA 2018, zmieniony przez pkt 3 ppkt 3 załącznika 8 do ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁴⁷⁾ Wprowadzonym pkt 4 ppkt 2 załącznika 8 do ustawy o wykorzystaniu danych i dostępie do danych.

w art. 74AB ust. 2 DPA 2018 zawarto niewyczerpujący wykaz elementów, które należy uwzględnić przy ocenie, czy warunki testu zostały spełnione, takich jak poszanowanie praworządności i praw człowieka, istnienie i uprawnienia organu ochrony danych, ustalenia dotyczące sądowych lub pozasądowych środków zaskarżenia, przepisy dotyczące przekazywania danych osobowych z państwa otrzymującego dane lub przez organizację otrzymującą dane do innych państw lub organizacji międzynarodowych, odpowiednie zobowiązania międzynarodowe tego państwa lub tej organizacji oraz konstytucja, tradycja i kultura tego państwa lub tej organizacji. Chociaż nowy przepis stanowi przeformułowanie wykazu istotnych elementów przewidzianych w dawnym art. 74 A DPA 2018, zachowuje on podstawowe elementy tego wykazu i w związku z tym pozostaje zbliżony do tego, co przewidziano w art. 36 dyrektywy (UE) 2016/680. Ponadto władze Zjednoczonego Królestwa potwierdziły, że Sekretarz Stanu będzie uwzględniać elementy niewymienione w art. 74AB ust. 2, takie jak przepisy ustawowe i praktyki państwa trzeciego w zakresie sposobu, w jaki organy publiczne uzyskują dostęp do danych osobowych do celów takich jak bezpieczeństwo narodowe lub ściganie przestępstw, w zakresie, w jakim mają one wpływ na ogólny standard ochrony. Oprócz tego, władze Zjednoczonego Królestwa uważają odpowiednie orzecznictwo państwa trzeciego za kluczowy element rozpatrywania kwestii wymienionych w sposób niewyczerpujący w art. 74AB ust. 2 DPA 2018.

- (38) Rozporządzenia zatwierdzające przekazanie danych nadal podlegają „ogólnym” wymogom proceduralnym przewidzianym w art. 182 DPA 2018, jak określono w motywie 77 decyzji wykonawczej (UE) 2021/1773. W ramach tej procedury Sekretarz Stanu musi przeprowadzić konsultacje z Komisarzem ds. Informacji, gdy proponuje przyjęcie rozporządzenia Zjednoczonego Królestwa stwierdzającego odpowiedni stopień ochrony⁽⁴⁸⁾. Po przyjęciu przez Sekretarza Stanu rozporządzenie takie jest przedkładane parlamentowi i podlega procedurze odrzucenia przez obie izby parlamentu (ang. *negative resolution*), w ramach której obie izby parlamentu mogą poddać rozporządzenie kontroli i mają możliwość przyjęcia wniosku o jego unieważnienie w ciągu 40 dni⁽⁴⁹⁾.
- (39) Art. 75 DPA 2018, zmieniony pkt 6 załącznika 8 do ustawy o wykorzystaniu danych i dostępie do danych, w odniesieniu do odpowiednich zabezpieczeń stanowi, że takie przekazywanie danych może mieć miejsce wyłącznie wtedy, gdy: a) zamierzony odbiorca danych jest związany odpowiednim instrumentem prawnym, tj. instrumentem spełniającym warunki określone w nowo dodanym ust. 4, w szczególności warunek polegający na tym, że każdy właściwy organ Zjednoczonego Królestwa będący stroną takiego instrumentu, działając w sposób racjonalny i proporcjonalny, uznaje, że warunki testu ochrony danych zostały spełnione, lub gdy b) administrator, działając w sposób racjonalny i proporcjonalny, uznaje, że warunki testu ochrony danych zostały spełnione w odniesieniu do konkretnego przekazania lub rodzaju przekazania. W nowo dodanym art. 75 ust. 5 DPA 2018 wyjaśniono, że warunki testu ochrony danych są spełnione, jeżeli ze względu na wymagane zabezpieczenia standard ochrony zapewniany osobom, których dane dotyczą, nie jest po przekazaniu znacznie niższy niż standard określony w odpowiednich przepisach Zjednoczonego Królestwa o ochronie danych. Przepisy te są zbliżone do środków określonych w art. 37 dyrektywy (UE) 2016/680. W związku z tym w UE i Zjednoczonym Królestwie obowiązują te same normy prawne dotyczące zatwierdzania przekazania danych z zastrzeżeniem odpowiednich zabezpieczeń. Zgodnie z nowo dodanym art. 75 ust. 6 DPA 2018 to, co jest rozsądne i proporcjonalne, należy ustalić na podstawie wszystkich okoliczności lub prawdopodobnych okoliczności danego przekazania lub rodzaju przekazania, w tym charakteru i ilości przekazywanych danych osobowych.
- (40) Jeżeli chodzi o przekazywanie danych na podstawie szczególnych okoliczności zgodnie z art. 76 DPA 2018, wprowadzono szereg zmian formalnych, które doprecyzowują warunki, na których takie przekazywanie może się odbywać, ale które nie wpływają na stopień ochrony danych osobowych w Zjednoczonym Królestwie⁽⁵⁰⁾.
- (41) Jeżeli chodzi o wdrażanie przepisów Zjednoczonego Królestwa dotyczących międzynarodowego przekazywania danych, od czasu przyjęcia decyzji wykonawczej (UE) 2021/1773 nastąpił szereg zmian.
- (42) Po pierwsze, po zawarciu w 2022 r. protokołu ustaleń między Ministerstwem Spraw Wewnętrznych a Komisarzem ds. Informacji, w którym określono ich odpowiednie role w przeprowadzaniu ocen odpowiedniego stopnia ochrony w dziedzinie ścigania przestępstw⁽⁵¹⁾, Zjednoczone Królestwo przeprowadziło oceny ram ochrony danych

⁽⁴⁸⁾ Zob. protokół ustaleń między Sekretarzem Stanu Departamentu Cyfryzacji, Kultury, Mediów i Sportu (DCMS) a Biurem Komisarza ds. Informacji w sprawie roli Biura w ponownej ocenie, czy Zjednoczone Królestwo zapewnia odpowiedni stopień ochrony, dostępny pod następującym adresem: <https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments>.

⁽⁴⁹⁾ W przypadku przyjęcia takiego wniosku w drodze głosowania rozporządzenie ostatecznie przestanie wywoływać jakiejkolwiek dalsze skutki prawne.

⁽⁵⁰⁾ Pkt 7 załącznika 8 do ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁵¹⁾ Dostęp pod adresem: <https://ico.org.uk/media2/about-the-ico/mou/4025752/ico-ho-mou.pdf>.

w Baliwatach Jersey i Guernsey, a także na Wyspie Man. W rezultacie w lipcu 2023 r. Zjednoczone Królestwo przyjęło rozporządzenie stwierdzające odpowiedni stopień ochrony dla Guernsey ⁽⁵²⁾, w listopadzie 2023 r. dla Jersey ⁽⁵³⁾, a w styczniu 2025 r. dla Wyspy Man ⁽⁵⁴⁾. Rozporządzenia te potwierdzają, że każda z tych jurysdykcji zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych na podstawie części 3 DPA 2018. Chociaż rozporządzenia te pierwotnie przyjęto na podstawie poprzednich ram prawnych, ocena leżąca u ich podstaw pozostaje ważna w zaktualizowanych ramach prawnych. W rezultacie rozporządzenia te nadal ułatwiają współpracę międzynarodową w dziedzinie ścigania przestępstw.

- (43) Oceniając funkcjonowanie decyzji stwierdzających odpowiedni stopień ochrony, przyjętych na podstawie art. 25 ust. 6 dyrektywy 95/46/WE zgodnie z art. 97 rozporządzenia (UE) 2016/679, Komisja oceniła również ramy ochrony danych w przypadku przetwarzania danych osobowych w kontekście ścigania przestępstw, a także zasady dostępu organów publicznych do danych osobowych do celów bezpieczeństwa narodowego w Baliwatach Jersey i Guernsey oraz na Wyspie Man. Między innymi na podstawie tej oceny Komisja stwierdziła, że wszystkie trzy jurysdykcje nadal zapewniają odpowiedni poziom ochrony danych osobowych przekazywanych z UE ⁽⁵⁵⁾.
- (44) Po drugie, w 2022 r. Zjednoczone Królestwo i Stany Zjednoczone zawarły umowę o ochronie danych i prywatności między Zjednoczonym Królestwem a Stanami Zjednoczonymi ⁽⁵⁶⁾, która stosuje odpowiednio warunki umowy ramowej między UE a USA ⁽⁵⁷⁾, zapewniając równoważną ochronę w kontekście wymiany danych między Zjednoczonym Królestwem a Stanami Zjednoczonymi do celów ścigania przestępstw.
- (45) Po trzecie, w 2023 r. i 2025 r. Komisarz ds. Informacji zaktualizował swoje wytyczne dotyczące międzynarodowego przekazywania danych na podstawie części 3 rozdział 5 DPA 2018 ⁽⁵⁸⁾. W aktualizacji z 2023 r. wyjaśniono znaczenie wymogu „ściślej niezbędności” przekazywania danych odbiorcom innym niż odpowiednie organy ścigania, dając tym samym administratorom danych większą pewność oceny legalności takiego przekazywania danych. W 2025 r. wykaz odpowiednich państw i terytoriów zaktualizowano w następstwie wydania przez Zjednoczone Królestwo rozporządzenia stwierdzającego odpowiedni stopień ochrony na Wyspie Man.

2.2.4. Zautomatyzowane podejmowanie decyzji

- (46) Mimo że przyjmując ustawę o wykorzystaniu danych i dostępie do danych, zachowano liczne elementy przepisów dotyczących zautomatyzowanego podejmowania decyzji ocenionych w motywach 72 i 73 decyzji wykonawczej (UE) 2021/1773, zmieniono nią niektóre aspekty tych przepisów.
- (47) Po pierwsze, w nowo wprowadzonym art. 50B DPA 2018 ustanowiono ogólny zakaz podejmowania istotnych decyzji w oparciu w całości lub w części o przetwarzanie szczególnych kategorii danych osobowych. Określono w nim jednak dwa wyjątki od tego zakazu, mające zastosowanie, gdy: osoba, której dane dotyczą, wyraziła wyraźną zgodę na takie przetwarzanie lub decyzja jest wymagana lub dozwolona przez prawo ⁽⁵⁹⁾.
- (48) Po drugie, w nowo wprowadzonym art. 50C DPA 2018 zobowiązano administratorów do wdrożenia zabezpieczeń w odniesieniu do wszelkich istotnych decyzji opartych w całości lub w części na danych osobowych i opartych wyłącznie na zautomatyzowanym przetwarzaniu. Zabezpieczenia te muszą obejmować przekazywanie osobie,

⁽⁵²⁾ Dostęp pod adresem: <https://www.legislation.gov.uk/uksi/2023/1221/contents/made>.

⁽⁵³⁾ Dostęp pod adresem: <https://www.legislation.gov.uk/uksi/2023/744/made>.

⁽⁵⁴⁾ Dostęp pod adresem: <https://www.legislation.gov.uk/uksi/2025/89/contents/made>.

⁽⁵⁵⁾ Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie pierwszego przeglądu decyzji stwierdzających odpowiedni stopień ochrony, które przyjęto na podstawie art. 25 ust. 6 dyrektywy 95/46/WE z dnia 15 stycznia 2024 r., dostępne pod adresem: <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52024DC0007>; oraz sprawozdania krajowe w sprawie funkcjonowania decyzji stwierdzających odpowiedni stopień ochrony przyjętych na podstawie dyrektywy 95/46/WE towarzyszące sprawozdaniu Komisji dla Parlamentu Europejskiego i Rady w sprawie pierwszego przeglądu decyzji stwierdzających odpowiedni stopień ochrony, które przyjęto na podstawie art. 25 ust. 6 dyrektywy 95/46/WE, dostępne pod adresem: https://commission.europa.eu/document/download/f8229eb2-1a36-4cf5-a099-1cd001664bff_en?filename=JUST_template_comingsoon_Commission%20Staff%20Working%20Document%20-%20Report%20on%20the%20first%20review%20of%20the%20functioning.pdf.

⁽⁵⁶⁾ Dostęp pod adresem: <https://www.gov.uk/government/publications/uk-usa-exchange-of-notes-on-the-protection-of-personal-information-relating-to-prevention-investigation-detection-and-prosecution-of-criminal-offences>.

⁽⁵⁷⁾ Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych (Dz.U. L 336 z 10.12.2016, s. 3), dostępna pod adresem: [https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:22016A1210\(01\)&from=PL](https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:22016A1210(01)&from=PL).

⁽⁵⁸⁾ Dostęp pod adresem: <https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/international-transfers/>.

⁽⁵⁹⁾ Art. 50B DPA 2018, wprowadzony art. 80 ust. 3 ustawy o wykorzystaniu danych i dostępie do danych.

której dane dotyczą, informacji na temat procesu decyzyjnego, umożliwienie tej osobie zakwestionowania decyzji lub złożenia oświadczeń oraz zapewnienie jej możliwości zażądania udziału człowieka w procesie decyzyjnym⁽⁶⁰⁾. Wprawdzie w art. 50C ust. 4 DPA 2018 przewidziano wyłączenie stosowania tych zabezpieczeń, gdy jest to konieczne, aby uniknąć utrudniania postępowania przygotowawczego lub procedury urzędowej, uniknąć negatywnego wpływu na zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych i wykonywanie kar, chronić bezpieczeństwo publiczne, bezpieczeństwo narodowe lub prawa i wolności innych osób, jednak stosowanie tych zabezpieczeń zawiesza się wówczas jedynie tymczasowo, biorąc pod uwagę fakt, że administrator jest zobowiązany do ponownego rozpatrzenia decyzji tak szybko, jak to możliwe, oraz że ponowne rozpatrzenie decyzji wymaga znaczącego zaangażowania człowieka⁽⁶¹⁾.

- (49) Ponadto w nowym art. 50 A DPA 2018 wyjaśniono definicję decyzji „opartej wyłącznie na zautomatyzowanym przetwarzaniu”, stanowiąc, że jest to decyzja, w przypadku której nie ma znaczącego zaangażowania człowieka w proces decyzyjny. Co ważne, administratorzy są zobowiązani do oceny, w jakim stopniu profilowanie przyczynia się do decyzji w sprawie ustalenia, czy zaangażowanie człowieka było znaczące. W art. 50 A DPA 2018 wyjaśniono również, że „istotna decyzja” to decyzja, która wywołuje negatywne skutki prawne lub podobnie znaczące negatywne skutki dla osoby, której dane dotyczą⁽⁶²⁾. To ograniczenie do decyzji, które mają niekorzystny wpływ na osobę, której dane dotyczą, odzwierciedla fakt, że – w przeciwieństwie do przetwarzania danych na podstawie RODO UK – jest mało prawdopodobne, aby właściwe organy podjęły jakąkolwiek decyzję, którą osoba, której dane dotyczą, uznałaby za pozytywną.
- (50) Ponadto w nowo wprowadzonym art. 50D DPA 2018 przyznano Sekretarzowi Stanu uprawnienia do wydawania aktów wykonawczych w celu opisanie, co stanowi znaczące zaangażowanie człowieka, a co nie, oraz jakie decyzje uznaje się za mające podobnie znaczące negatywne skutki dla osoby, której dane dotyczą, a jakich nie. Nowy przepis umożliwia również Sekretarzowi Stanu wydawanie aktów wykonawczych w celu (i) dodania nowych zabezpieczeń; (ii) nałożenia wymogów uzupełniających istniejące zabezpieczenia; oraz (iii) określenia środków, które nie spełniają tych zabezpieczeń⁽⁶³⁾. Co ważne, przed przyjęciem nowego rozporządzenia zgodnie z art. 50D DPA 2018 Sekretarz Stanu musi skonsultować się z Komisarzem ds. Informacji⁽⁶⁴⁾, a rozporządzenie takie podlega procedurze zatwierdzenia (ang. *affirmative resolution*)⁽⁶⁵⁾, co oznacza, że do jego przyjęcia wymagane jest zatwierdzenie przez obie izby parlamentu Zjednoczonego Królestwa.
- (51) Ustawą o wykorzystaniu danych i dostępie do danych zmieniono wprawdzie tym samym ramy zautomatyzowanego podejmowania decyzji, jednak należy zauważyć, że zgodnie z ramami prawnymi Zjednoczonego Królestwa zautomatyzowane podejmowanie decyzji nadal podlega kluczowemu zabezpieczeniu wymagającemu prawa do uzyskania interwencji ludzkiej we wszystkich przypadkach zautomatyzowanego podejmowania decyzji, tj. na podstawie przetwarzania wrażliwych i niewrażliwych danych osobowych⁽⁶⁶⁾.

2.2.5. Rozliczalność

- (52) W ramach prawnych Zjednoczonego Królestwa nadal przestrzega się zasady rozliczalności przewidzianej w dyrektywie (UE) 2016/680, zobowiązującej organy publiczne do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia i wykazania zgodności z obowiązkami w zakresie ochrony danych, jak oceniono w motywach 88–92 decyzji wykonawczej (UE) 2021/1773.
- (53) Jednym ze środków zawartych w DPA 2018 w celu zapewnienia rozliczalności oraz umożliwienia administratorom i podmiotom przetwarzającym wykazania zgodności jest wymóg, aby właściwe organy prowadziły rejestry swoich czynności przetwarzania, w tym zbierania, modyfikowania, przeglądania, ujawniania, łączenia i usuwania danych osobowych⁽⁶⁷⁾. Ustawa o wykorzystaniu danych i dostępie do danych zmienia szczególne obowiązki administratorów wynikające z tego przepisu, usuwając tylko z art. 62 DPA 2018 wymóg rejestrowania przez administratorów uzasadnienia w przypadku przeglądania lub ujawniania danych osobowych⁽⁶⁸⁾. Co ważne, sam wymóg rejestrowania przez administratorów czynności przetwarzania nadal obowiązuje, co oznacza, że zachowano główny mechanizm zapewniania rozliczalności.

⁽⁶⁰⁾ Art. 50C DPA 2018, wprowadzony art. 80 ust. 3 ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁶¹⁾ Art. 50C ust. 3 i 4 DPA 2018, wprowadzone art. 80 ust. 3 ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁶²⁾ Art. 50 A DPA 2018, wprowadzony art. 80 ust. 3 ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁶³⁾ Art. 50D DPA 2018, wprowadzony art. 80 ust. 3 ustawy o wykorzystaniu danych i dostępie do danych. Wszelkie rozporządzenia wydane w ramach tych uprawnień podlegają procedurze zatwierdzenia przez obie izby parlamentu (ang. *affirmative resolution*), co zapewnia nadzór parlamentarny. Rozporządzenia te nie mogą zmieniać wymogów określonych w art. 50C.

⁽⁶⁴⁾ Art. 182 ust. 2 DPA 2018.

⁽⁶⁵⁾ Art. 50D ust. 5 DPA 2018.

⁽⁶⁶⁾ Art. 50C ust. 2 lit. c) DPA 2018.

⁽⁶⁷⁾ Art. 62 DPA 2018. Zob. także motyw 90 decyzji wykonawczej (UE) 2021/1773.

⁽⁶⁸⁾ Art. 82 ustawy o wykorzystaniu danych i dostępie do danych.

2.3. Nadzór i egzekwowanie przepisów

2.3.1. Niezależny nadzór

- (54) W Zjednoczonym Królestwie nadzór i egzekwowanie zgodności z ramami ochrony danych nadal sprawuje niezależny organ nadzorczy odpowiedzialny za ochronę danych, jak przeanalizowano w motywach 93–99 decyzji wykonawczej (UE) 2021/1773. W ustawie o wykorzystaniu danych i dostępie do danych zreformowano strukturę zarządzania tego organu, ustanawiając podmiot posiadający osobowość prawną – Komisję ds. Informacji – zastępujący Komisarza ds. Informacji, który był organem jednoosobowym z osobowością prawną.
- (55) Wdrożenie środków określonych w ustawie o wykorzystaniu danych i dostępie do danych będzie więc oznaczało zlikwidowanie urzędu Komisarza ds. Informacji i przeniesienie funkcji, personelu i mienia tego organu do nowego organu – Komisji ds. Informacji. Komisja ds. Informacji będzie się składać z członków wykonawczych i niewykonawczych⁽⁶⁹⁾. Ustawa przewiduje również możliwość, aby w okresie przejściowym Komisarz ds. Informacji objął funkcje przewodniczącego Komisji ds. Informacji, będącego jednym z jej członków niewykonawczych⁽⁷⁰⁾. Ustawa o wykorzystaniu danych i dostępie do danych stanowi ponadto, że w zakresie, w jakim jest to odpowiednie w wyniku przekazania funkcji, odniesienia do Komisarza ds. Informacji we wszystkich aktach normatywnych lub innych dokumentach (o ile zostały one przyjęte lub sporządzone) należy traktować jako odniesienia do Komisji ds. Informacji. W celu wykonywania swoich funkcji Komisja może ustanawiać komitety i powierzać funkcje swoim poszczególnym członkom, pracownikom lub komitetom⁽⁷¹⁾ oraz może przyjmować regulaminy Komisji i komitetów, w tym w odniesieniu do quorum i podejmowania decyzji większością głosów. Regulaminy takie muszą zostać podane do wiadomości publicznej⁽⁷²⁾.
- (56) Co ważne, niezależność Komisji ds. Informacji podlega takim samym zabezpieczeniom, w tym w odniesieniu do przepisów dotyczących powoływania i odwoływania przewodniczącego, jak te ocenione w motywach 95–98 decyzji wykonawczej (UE) 2021/1773⁽⁷³⁾. Podobne środki ochrony mają zastosowanie do pozostałych członków niewykonawczych Komisji ds. Informacji. W szczególności przewodniczący Komisji ds. Informacji jest powoływany przez Jego Królewską Mość na zalecenie Sekretarza Stanu. Jest on wybierany na podstawie osiągnięć, w drodze sprawiedliwego i otwartego konkursu⁽⁷⁴⁾. Pozostali członkowie niewykonawczy są powoływani przez Sekretarza Stanu po konsultacji z przewodniczącym. Zalecenie powołania lub powołanie jest możliwe tylko wobec kandydatów, którzy zostali wybrani na podstawie osiągnięć, w drodze sprawiedliwego i otwartego konkursu, oraz jeżeli Sekretarz Stanu jest przekonany, że nie znajdują się oni w sytuacji konfliktu interesów⁽⁷⁵⁾. Członkowie wykonawczy są pracownikami Komisji ds. Informacji zatrudnionymi na zasadach i warunkach określonych przez członków niewykonawczych⁽⁷⁶⁾. Dyrektor wykonawczy jest powoływany przez przewodniczącego i innych członków niewykonawczych po konsultacji z Sekretarzem Stanu. Członkowie wykonawczy również są wybierani na podstawie osiągnięć, w drodze sprawiedliwego i otwartego konkursu⁽⁷⁷⁾.
- (57) Przewodniczący może zostać odwołany ze stanowiska wyłącznie przez Jego Królewską Mość na podstawie oświadczenia obu izb parlamentu i tylko wtedy, gdy Sekretarz Stanu przedstawi izbie sprawozdanie, w którym wyrazi przekonanie, że przewodniczący jest winny poważnego uchybienia, znajduje się w konflikcie interesów, nie spełnił szczegółowych wymogów informacyjnych w odniesieniu do potencjalnych konfliktów interesów lub nie jest w stanie, nie jest zdolny lub nie chce pełnić swoich funkcji⁽⁷⁸⁾. Sekretarz Stanu może odwołać członka niewykonawczego ze stanowiska tylko wówczas, gdy jest przekonany o spełnieniu szczególnych warunków określonych w przepisach. Warunki te obejmują konflikt interesów, poważne uchybienie oraz niezdolność, niechęć lub niezdadność do wykonywania swoich obowiązków. Jeżeli chodzi o dodatkowe zabezpieczenia, Sekretarz Stanu ma obowiązek podać do wiadomości publicznej decyzję w tej sprawie i przedstawić odwołanemu członkowi uzasadnienie jego odwołania⁽⁷⁹⁾.

⁽⁶⁹⁾ Pkt 3 ppkt 1 załącznika 12 A do DPA 2018.

⁽⁷⁰⁾ Art. 117, 118, 119 i 120 wraz z załącznikiem 14 do ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁷¹⁾ Pkt 13 i 14 załącznika 12 A do DPA 2018.

⁽⁷²⁾ Pkt 16 załącznika 12 A do DPA 2018.

⁽⁷³⁾ Art. 52 RODO UK, a także załącznik 12 A do DPA 2018, wprowadzony art. 117 ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁷⁴⁾ Pkt 5 ppkt 1 załącznika 12 A do DPA 2018.

⁽⁷⁵⁾ Pkt 3 ppkt 2, pkt 5 i pkt 6 załącznika 12 A do DPA 2018.

⁽⁷⁶⁾ Pkt 11 załącznika 12 A do DPA 2018.

⁽⁷⁷⁾ Pkt 5 ppkt 2 załącznika 12 A do DPA 2018.

⁽⁷⁸⁾ Pkt 7 ppkt 6 i 7 załącznika 12 A do DPA 2018.

⁽⁷⁹⁾ Pkt 9 ppkt 6, 7, 8 i 9 załącznika 12 A do DPA 2018.

- (58) Ustawa o wykorzystaniu danych i dostępie do danych nie zmienia podstawowych obowiązków Komisji ds. Informacji, która nadal będzie pełnić funkcje określone w załączniku 13 do DPA 2018. Obejmują one monitorowanie i egzekwowanie przestrzegania części 3 DPA 2018, doradzanie parlamentowi i rządowi, podnoszenie świadomości społecznej, wspieranie administratorów danych i podmiotów przetwarzających w wypełnianiu ich obowiązków oraz informowanie osób fizycznych o przysługujących im prawach⁽⁸⁰⁾. W ustawie o wykorzystaniu danych i dostępie do danych wyjaśniono, że wykonując obowiązek zapewnienia odpowiedniego stopnia ochrony danych osobowych, Komisja ds. Informacji będzie musiała brać pod uwagę interesy osób, których dane dotyczą, administratorów i innych podmiotów, uwzględniać szerszy interes publiczny oraz propagować zaufanie publiczne do przetwarzania danych osobowych⁽⁸¹⁾.
- (59) Ponadto w ustawie o wykorzystaniu danych i dostępie do danych określono, że podczas wykonywania swoich funkcji na mocy przepisów o ochronie danych, w zakresie, w jakim jest to istotne w danych okolicznościach, Komisja ds. Informacji uwzględni kwestię propagowania innowacji i konkurencji, znaczenie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych oraz wykrywania i ścigania czynów zabronionych, potrzebę ochrony bezpieczeństwa publicznego i bezpieczeństwa narodowego oraz szczególne potrzeby związane z ochroną dzieci⁽⁸²⁾. Prawo UE o ochronie danych również uznaje potrzebę równoważenia ochrony danych osobowych z szeregiem innych praw podstawowych oraz celów, takich jak bezpieczeństwo i sprawiedliwość⁽⁸³⁾.

2.3.2. Egzekwowanie przepisów, w tym sankcje, i środki zaskarżenia

- (60) Uprawnienia i zadania Komisji ds. Informacji nadal odpowiadają uprawnieniom i zadaniom organów nadzorczych odpowiedzialnych za ochronę danych państw członkowskich zgodnie z odpowiednimi artykułami dyrektywy (UE) 2016/680⁽⁸⁴⁾, jak oceniono w motywach 100–109 decyzji wykonawczej (UE) 2021/1773.
- (61) Ustawą o wykorzystaniu danych i dostępie do danych wprowadzono pewne wyjaśnienia dotyczące wykonywania niektórych z tych uprawnień.
- (62) Art. 97 ustawy o wykorzystaniu danych i dostępie do danych zmieniono art. 142 DPA 2018, aby wyraźnie umożliwić Komisji ds. Informacji żądanie nie tylko informacji, ale również konkretnych dokumentów, zwiększając jej zdolność do badania i weryfikacji zgodności.
- (63) Art. 98 ustawy o wykorzystaniu danych i dostępie do danych wzmacnia uprawnienia Komisji ds. Informacji na mocy art. 146 DPA 2018 przez umożliwienie Komisji ds. Informacji zażądania od administratora danych lub podmiotu przetwarzającego zlecenia niezależnego sprawozdania w określonej sprawie. Sprawozdanie musi przygotować „zatwierdzona osoba”, przy czym Komisja ds. Informacji jest uprawniona do ostatecznego zatwierdzenia kandydata lub wyznaczenia osoby, jeżeli nie zaproponowano żadnego odpowiedniego kandydata lub jeżeli administrator danych nie podejmie działań⁽⁸⁵⁾. W zawiadomieniu oceniającym można określić format, treść i termin sprawozdania⁽⁸⁶⁾. Wszelkie powiązane koszty, w tym wynagrodzenie zatwierdzonej osoby, musi pokryć administrator lub podmiot przetwarzający⁽⁸⁷⁾.
- (64) W art. 100 ustawy o wykorzystaniu danych i dostępie do danych ustanowiono nowe narzędzie egzekwowania prawa na podstawie art. 148 A DPA 2018; jest nim wezwanie na przesłuchanie. Komisja ds. Informacji może wymagać od osób fizycznych udziału w przesłuchaniach przy zastosowaniu zabezpieczeń takich jak ochrona przed samooskarżeniem i prawnicza tajemnica zawodowa⁽⁸⁸⁾.
- (65) Art. 101 ustawy o wykorzystaniu danych i dostępie do danych zmieniono załącznik 16 DPA 2018, aby zapewnić Komisji ds. Informacji większą elastyczność w wydawaniu zawiadomień w sprawie sankcji. Chociaż ogólną zasadą pozostaje obecny sześciomiesięczny termin na wydanie ostatecznego zawiadomienia w sprawie sankcji po ogłoszeniu zamiaru, przepis ten zezwala Komisji ds. Informacji na wydanie zawiadomienia w sprawie sankcji po upływie tego terminu, jeżeli dotrzymanie terminu nie jest racjonalnie wykonalne. W takich przypadkach zawiadomienie należy wydać tak szybko, jak to możliwe. Ponadto, w przypadku gdy Komisja ds. Informacji postanowi nie wydawać zawiadomienia w sprawie sankcji, musi poinformować o tym zainteresowaną osobę na piśmie w terminie sześciu miesięcy lub tak szybko, jak to możliwe po upływie tego terminu. Artykuł ten wprowadza również nowy wymóg, aby Komisja ds. Informacji publikowała wytyczne dotyczące okoliczności, w których wydanie zawiadomienia w sprawie sankcji może wymagać ponad sześciu miesięcy.

⁽⁸⁰⁾ Załącznik 13 do DPA 2018.

⁽⁸¹⁾ Art. 91 ustawy o wykorzystaniu danych i dostępie do danych, wprowadzający art. 120 A DPA 2018.

⁽⁸²⁾ Art. 91 ustawy o wykorzystaniu danych i dostępie do danych, wprowadzający art. 120B DPA 2018.

⁽⁸³⁾ Zob. w szczególności motyw 2 dyrektywy (UE) 2016/680.

⁽⁸⁴⁾ Pkt 2 załącznika 13 do DPA 2018.

⁽⁸⁵⁾ Art. 98 ustawy o wykorzystaniu danych i dostępie do danych, wprowadzający art. 146 A DPA 2018.

⁽⁸⁶⁾ Art. 98 ustawy o wykorzystaniu danych i dostępie do danych, wprowadzający art. 146 ust. 3 A DPA 2018.

⁽⁸⁷⁾ Art. 98 ustawy o wykorzystaniu danych i dostępie do danych, wprowadzający art. 146 ust. 11 A DPA 2018.

⁽⁸⁸⁾ Art. 98 ustawy o wykorzystaniu danych i dostępie do danych, wprowadzający art. 146 ust. 8B DPA 2018.

- (66) Art. 102 ustawy o wykorzystaniu danych i dostępie do danych wprowadzono nowe obowiązki sprawozdawcze Komisji ds. Informacji. Artykułem tym zmieniono art. 139 i dodano nowy art. 161 A do DPA 2018, zobowiązujący Komisję ds. Informacji do publikowania rocznego sprawozdania z działań regulacyjnych. W tym sprawozdaniu należy szczegółowo opisać, w jaki sposób wykonano uprawnienia dochodzeniowe i wykonawcze wynikające z RODO UK oraz części 3 i 4 DPA 2018. Musi ono również ujawnić liczbę zawiadomień w sprawie sankcji wydanych po upływie sześciomiesięcznego terminu po ogłoszeniu zamiaru oraz przedstawić uzasadnienie opóźnienia. Ponadto w sprawozdaniu należy wyjaśnić, w jaki sposób Komisja ds. Informacji zastosowała się do własnych wytycznych przy podejmowaniu decyzji regulacyjnych.
- (67) Art. 103 ustawy o wykorzystaniu danych i dostępie do danych wzmacnia procedurę składania skarg dostępną dla osób, których dane dotyczą. Wprowadza on do DPA 2018 nowe art. 164 A i 164B. Art. 164 A stanowi, że osoby, których dane dotyczą, mają prawo wnosić skargi bezpośrednio do administratorów danych, jeżeli uważają, że ich prawa wynikające z RODO UK lub części 3 DPA 2018 zostały naruszone. Administratorzy muszą ułatwiać ten proces, uznawać skargi w ciągu 30 dni i udzielać odpowiedzi bez zbędnej zwłoki. Muszą również na bieżąco informować skarżących o postępach i wynikach. Art. 164B przyznaje Sekretarzowi Stanu uprawnienie do wydawania rozporządzeń nakładających na administratorów obowiązek zgłaszania liczby otrzymanych skarg.
- (68) Art. 104 ustawy o wykorzystaniu danych i dostępie do danych wprowadza do DPA 2018 nowy art. 180 A w celu wyjaśnienia uprawnień sądu w postępowaniu w sprawie żądania udzielania dostępu przez osoby, których dane dotyczą. Zgodnie z tym przepisem sądy mogą wymagać, aby administratorzy danych przekazywali sporne informacje do celów ich zbadania przez sąd przy podejmowaniu decyzji, czy osoba, której dane dotyczą, jest do nich uprawniona. Informacji nie można jednak ujawniać osobie, której dane dotyczą, o ile sąd nie stwierdzi, że ma ona prawo dostępu do nich. Artykuł ten wyjaśnia, że sądy mają możliwość badania spornych materiałów bez wcześniejszego ujawniania ich powodowi, przywracając zabezpieczenie, które istniało wcześniej na mocy ustawy o ochronie danych z 1998 r.
- (69) Jeżeli chodzi o wykonywanie tych uprawnień, od czasu przyjęcia decyzji wykonawczej (UE) 2021/1773 Komisarz ds. Informacji rozpatrzył liczne skargi⁽⁸⁹⁾ oraz przeprowadził szereg dochodzeń i zastosował środki egzekucyjne w odniesieniu do przetwarzania danych przez organy ścigania. W latach 2021–2025 Komisarz ds. Informacji prowadził dochodzenia i wydał nagany wobec różnych organów policji za różne przypadki niewywiązywania się z obowiązków w zakresie ochrony danych, na przykład przy odpowiadaniu na żądania udzielenia dostępu do danych, przy stosowaniu środków bezpieczeństwa w odniesieniu do danych z monitoringu wizyjnego, przy zajmowaniu się szczególnie chronionymi rejestrami karnymi, przy łączeniu danych różnych osób lub przy ujawnianiu danych osobowych osobom trzecim⁽⁹⁰⁾. Komisarz ds. Informacji wydawał również i aktualizował wytyczne i opinie, na przykład dotyczące prawa dostępu lub sposobu rozpatrywania żądań w sposób oczywisty nieuzasadnionych lub nadmiernie wygórowanych na podstawie części 3 DPA 2018⁽⁹¹⁾, lub zaktualizował istniejące wytyczne, takie jak przewodnik dotyczący przetwarzania danych do celów ścigania przestępstw⁽⁹²⁾.

3. WNIOSKI

- (70) Komisja uważa, że część 3 DPA 2018 nadal zapewnia taki stopień ochrony danych osobowych przekazywanych do celów ścigania przestępstw z właściwych organów w Unii Europejskiej do właściwych organów w Zjednoczonym Królestwie, który jest merytorycznie równoważny stopniowi ochrony zagwarantowanemu w dyrektywie (UE) 2016/680.

⁽⁸⁹⁾ Na przykład w latach 2023–2024 do Komisji ds. Informacji wpłynęło 1 890 skarg na podstawie RODO lub DPA 2018 dotyczących organizacji w podsektorach „organ policji”, „siły policyjne” i „komisarze policji”. Zob. także sprawozdanie roczne i sprawozdanie finansowe Komisarza ds. Informacji za okres 2023–2024, dostępne pod adresem: <https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf>.

⁽⁹⁰⁾ Dodatkowe informacje są dostępne pod następującym adresem: <https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice>.

⁽⁹¹⁾ Dostęp pod adresem: <https://ico.org.uk/for-organisations/law-enforcement/the-right-of-access-part-3-of-the-dpa-2018/> i <https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/>.

⁽⁹²⁾ Dostęp pod adresem: <https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/>.

- (71) Ponadto Komisja stwierdza, że mechanizmy nadzoru i możliwości dochodzenia roszczeń przewidziane w prawie Zjednoczonego Królestwa – rozumiane jako całość – nadal zapewniają możliwość identyfikowania przypadków naruszenia przepisów i w praktyce nakładania za te naruszenia sankcji oraz oferują osobom, których dane dotyczą, możliwość skorzystania ze środków ochrony prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych, a także – ostatecznie – sprostowania lub usunięcia takich danych.
- (72) Należy zatem uznać, że Zjednoczone Królestwo nadal zapewnia odpowiedni stopień ochrony w rozumieniu art. 36 ust. 2 dyrektywy (UE) 2016/680, interpretowanego w świetle Karty praw podstawowych.

4. SKUTKI NINIEJSZEJ DECYZJI I DZIAŁANIA ORGANÓW OCHRONY DANYCH

- (73) Państwa członkowskie i ich organy mają obowiązek stosować środki niezbędne do zapewnienia zgodności z aktami instytucji unijnych, ponieważ domniemywa się, że akty te są zgodne z prawem, a zatem wywołują skutki prawne do chwili ich wygaśnięcia, uchylecia, stwierdzenia ich nieważności w postępowaniu o stwierdzenie nieważności lub orzeczenia o ich nieważności w następstwie odesłania prejudycjalnego lub zarzutu niezgodności z prawem.
- (74) Decyzja stwierdzająca odpowiedni stopień ochrony danych osobowych przyjęta przez Komisję na podstawie art. 36 ust. 3 dyrektywy (UE) 2016/680 jest zatem wiążąca dla wszystkich organów państw członkowskich, do których jest skierowana, w tym ich niezależnych organów nadzorczych. W szczególności w okresie stosowania decyzji wykonawczej (UE) 2021/1773 zmienionej niniejszą decyzją, przekazywanie danych przez administratora lub podmiot przetwarzający w Unii administratorom lub podmiotom przetwarzającym w Zjednoczonym Królestwie może odbywać się bez konieczności uzyskania jakiegokolwiek dodatkowego zezwolenia.
- (75) Należy przypomnieć, że zgodnie z art. 47 ust. 5 dyrektywy (UE) 2016/680 i jak wyjaśnił Trybunał Sprawiedliwości w wyroku w sprawie Schrems I, jeżeli krajowy organ ochrony danych kwestionuje, w tym na podstawie skargi, zgodność wydanej przez Komisję decyzji stwierdzającej odpowiedni stopień ochrony z przysługującymi osobie fizycznej prawami podstawowymi do prywatności i ochrony danych, należy zapewnić w prawie krajowym drogę prawną umożliwiającą jej podniesienie tych zarzutów przed sądem krajowym, który może być zobowiązany do wystąpienia z wnioskiem do Trybunału Sprawiedliwości o wydanie orzeczenia w trybie prejudycjalnym ⁽⁹³⁾.

5. MONITOROWANIE

- (76) Zgodnie z art. 36 ust. 4 dyrektywy (UE) 2016/680 Komisja jest zobowiązana na bieżąco monitorować odpowiednie zmiany w Zjednoczonym Królestwie, aby ocenić, czy nadal zapewnia ono merytorycznie równoważny stopień ochrony. Takie monitorowanie jest szczególnie ważne, ponieważ Zjednoczone Królestwo będzie stosować i egzekwować zmieniony system ochrony danych. Ponadto zmienione ramy ochrony danych Zjednoczonego Królestwa uprawniają Sekretarza Stanu do dalszego doprecyzowania tych ram w drodze aktów wykonawczych. W związku z tym należy zwrócić szczególną uwagę na takie dodatkowe doprecyzowania, a także na stosowanie w praktyce zmienionych przepisów Zjednoczonego Królestwa dotyczących przekazywania danych osobowych do państw trzecich, na skuteczność wykonywania praw indywidualnych – w tym wszelkie istotne zmiany w prawie i praktyce dotyczące nowo wprowadzonych wyjątków od takich praw lub ograniczeń takich praw – oraz na funkcjonowanie zrestrukturyzowanego urzędu Komisarza ds. Informacji, w tym w zakresie rozpatrywania skarg i stosowania uprawnień naprawczych. W monitorowaniu Komisja powinna uwzględniać między innymi zmiany w orzecznictwie oraz nadzór ze strony Komisarza ds. Informacji i innych niezależnych organów.
- (77) Aby ułatwić to monitorowanie, władze Zjednoczonego Królestwa powinny niezwłocznie i regularnie informować Komisję o wszelkich istotnych zmianach w porządku prawnym Zjednoczonego Królestwa, które mają wpływ na ramy prawne będące przedmiotem decyzji wykonawczej (UE) 2021/1773 zmienionej niniejszą decyzją, a także o wszelkich zmianach praktyk związanych z przetwarzaniem danych osobowych poddanych ocenie w decyzji wykonawczej (UE) 2021/1773 zmienionej niniejszą decyzją, w szczególności w odniesieniu do elementów, o których mowa w motywie (39).
- (78) Ponadto, aby Komisja mogła skutecznie realizować funkcję monitorowania, państwa członkowskie powinny informować ją o wszelkich istotnych działaniach podejmowanych przez organy ochrony danych państw członkowskich, zwłaszcza w odniesieniu do zapytań lub skarg osób z UE, których dane dotyczą, dotyczących przekazywania danych osobowych z Unii właściwym organom w Zjednoczonym Królestwie. Komisja powinna być również informowana o wszelkich sygnałach świadczących o tym, że działania organów publicznych Zjednoczonego Królestwa odpowiedzialnych za zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie czynów zabronionych, w tym wszelkich organów nadzoru, nie gwarantują wymaganego stopnia ochrony.

⁽⁹³⁾ Schrems I, pkt 65.

- (79) W przypadku gdy z dostępnych informacji, w szczególności informacji uzyskanych w wyniku monitorowania niniejszej decyzji lub przedstawionych przez władze Zjednoczonego Królestwa lub państw członkowskich, wynika, że stopień ochrony zapewniany przez Zjednoczone Królestwo może nie być już odpowiedni, Komisja powinna powiadomić o tym właściwe organy Zjednoczonego Królestwa i zwrócić się o zastosowanie właściwych środków w określonym terminie, który nie może przekraczać trzech miesięcy. W razie potrzeby okres ten może zostać przedłużony o określony czas, biorąc pod uwagę charakter danej kwestii i środki, które należy zastosować.
- (80) Jeżeli po upływie tego określonego terminu właściwe organy Zjednoczonego Królestwa nie stosują tych środków lub nie wykażą w inny zadowalający sposób, że niniejsza decyzja jest nadal oparta na odpowiednim stopniu ochrony, Komisja rozpocznie procedurę, o której mowa w art. 58 ust. 2 dyrektywy (UE) 2016/680, w celu częściowego lub całkowitego zawieszenia lub uchylecia niniejszej decyzji.
- (81) Ewentualnie Komisja rozpocznie tę procedurę w celu zmiany decyzji wykonawczej (UE) 2021/1773 zmienionej niniejszą decyzją, w szczególności uzależniając przekazywanie danych od spełnienia dodatkowych warunków lub ograniczając zakres stwierdzenia odpowiedniego stopnia ochrony wyłącznie do przekazywania danych, co do których zapewniono ciągłość odpowiedniego stopnia ochrony.
- (82) W należycie uzasadnionych, szczególnie pilnych przypadkach Komisja skorzysta z możliwości przyjęcia zgodnie z procedurą, o której mowa w art. 58 ust. 3 dyrektywy (UE) 2016/680, mających natychmiastowe zastosowanie aktów wykonawczych zawieszających, uchylających lub zmieniających decyzję.

6. PRZEGLĄD, OKRES OBOWIĄZYWANIA I PRZEDŁUŻENIE OBOWIĄZYWANIA NINIEJSZEJ DECYZJI

- (83) W zastosowaniu art. 36 ust. 3 dyrektywy (UE) 2016/680 oraz w świetle tego, że stopień ochrony zapewniany w ramach prawnych Zjednoczonego Królestwa może ulec zmianie, od czasu przyjęcia niniejszej decyzji Komisja powinna okresowo oceniać, czy ustalenia odnoszące się do adekwatności stopnia ochrony zapewnianego przez Zjednoczone Królestwo są nadal faktycznie i prawnie uzasadnione. Taką ocenę należy przeprowadzać co najmniej raz na cztery lata w odniesieniu do wszystkich aspektów obowiązywania niniejszej decyzji, w tym funkcjonowania odpowiednich mechanizmów nadzoru i egzekwowania.
- (84) W celu przeprowadzenia przeglądu Komisja powinna spotkać się z odpowiednimi przedstawicielami władz Zjednoczonego Królestwa, w tym z Komisją ds. Informacji. Uczestnictwo w tym spotkaniu powinno być otwarte dla przedstawicieli członków Europejskiej Rady Ochrony Danych. W ramach tego przeglądu Komisja powinna zwrócić się do Zjednoczonego Królestwa o przedłożenie wyczerpujących informacji o wszystkich aspektach istotnych dla stwierdzenia odpowiedniego stopnia ochrony. Komisja powinna również zwracać się o wyjaśnienia dotyczące wszelkich informacji istotnych dla niniejszej decyzji, w tym otrzymanych od EROD, poszczególnych organów ochrony danych i organizacji społeczeństwa obywatelskiego, a także informacji publicznie dostępnych, doniesień medialnych oraz informacji z innych dostępnych źródeł.
- (85) Na podstawie tej oceny Komisja powinna przygotować ogólnodostępne sprawozdanie, które przedłoży Parlamentowi Europejskiemu i Radzie.
- (86) Komisja musi również wziąć pod uwagę, że ramy ochrony danych ocenione w niniejszej decyzji i w decyzji wykonawczej (UE) 2021/1773 mogą ulec dalszym zmianom.
- (87) W związku z tym należy przewidzieć, że niniejsza decyzja będzie miała zastosowanie przez okres sześciu lat od chwili jej wejścia w życie.
- (88) W przypadku gdy w szczególności z informacji uzyskanych w wyniku monitorowania niniejszej decyzji będzie wynikało, że ustalenia dotyczące zapewniania w Zjednoczonym Królestwie odpowiedniego stopnia ochrony są nadal uzasadnione pod względem faktycznym i prawnym, Komisja powinna, najpóźniej sześć miesięcy przed zakończeniem okresu stosowania niniejszej decyzji, wszcząć procedurę zmiany niniejszej decyzji poprzez przedłużenie jej zakresu czasowego, co do zasady na dodatkowy okres czterech lat. Każdy taki akt wykonawczy zmieniający niniejszą decyzję należy przyjąć zgodnie z procedurą, o której mowa w art. 58 ust. 2 dyrektywy (UE) 2016/680.

7. UWAGI KOŃCOWE

- (89) Europejska Rada Ochrony Danych opublikowała swoją opinię⁽⁹⁴⁾, która została uwzględniona podczas przygotowywania niniejszej decyzji.
- (90) Środek przewidziany w niniejszej decyzji jest zgodny z opinią komitetu ustanowionego na mocy art. 58 dyrektywy (UE) 2016/680.
- (91) Zgodnie z art. 6a Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, który jest załączony do TUE i TFUE, Irlandia nie jest związana przepisami ustanowionymi w dyrektywie (UE) 2016/680, a zatem również w niniejszej decyzji wykonawczej, dotyczącymi przetwarzania danych osobowych przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres zastosowania części trzeciej tytuł V rozdział 4 lub 5 TFUE, jeżeli Irlandia nie jest związana zasadami regulującymi formy współpracy wymiarów sprawiedliwości w sprawach karnych lub współpracy policyjnej, w ramach której należy przestrzegać przepisów ustanowionych na podstawie art. 16 TFUE. Niemniej jednak na mocy decyzji wykonawczej Rady (UE) 2020/1745⁽⁹⁵⁾ przepisy dyrektywy (UE) 2016/680 zostały wprowadzone w życie i są tymczasowo stosowane w Irlandii od dnia 1 stycznia 2021 r. Irlandia jest zatem związana niniejszą decyzją na takich samych zasadach, jakie mają zastosowanie do stosowania dyrektywy (UE) 2016/680 w Irlandii, jak przewidziano w decyzji wykonawczej (UE) 2020/1745, jeżeli chodzi o tę część dorobku Schengen, w której uczestniczy.
- (92) Zgodnie z art. 2 i 2a Protokołu nr 22 w sprawie stanowiska Danii, który jest załączony do Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie jest związana przepisami ustanowionymi w dyrektywie (UE) 2016/680, a zatem również w niniejszej decyzji wykonawczej, dotyczącymi przetwarzania danych osobowych przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres zastosowania części trzeciej tytuł V rozdział 4 lub 5 TFUE, ani nie podlega stosowaniu tych przepisów. Biorąc jednak pod uwagę fakt, że dyrektywa (UE) 2016/680 opiera się na dorobku Schengen, zgodnie z art. 4 tego Protokołu w dniu 26 października 2016 r. Dania poinformowała o swojej decyzji dotyczącej wdrożenia dyrektywy (UE) 2016/680. W związku z powyższym na mocy prawa międzynarodowego Dania ma obowiązek wprowadzenia w życie przepisów niniejszej decyzji.
- (93) W odniesieniu do Islandii i Norwegii niniejsza decyzja stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy zawartej przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotyczącej włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen⁽⁹⁶⁾.
- (94) W odniesieniu do Szwajcarii niniejsza decyzja stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy zawartej między Unią Europejską, Wspólnotą Europejską a Konfederacją Szwajcarską w sprawie włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen⁽⁹⁷⁾.
- (95) W odniesieniu do Liechtensteinu niniejsza decyzja stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu w sprawie przystąpienia Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen⁽⁹⁸⁾.
- (96) Należy zatem odpowiednio zmienić decyzję wykonawczą (UE) 2021/1773,

⁽⁹⁴⁾ Opinia 27/2025 w sprawie projektu decyzji wykonawczej Komisji zmieniającej decyzję w sprawie odpowiedniej ochrony danych osobowych przez Zjednoczone Królestwo, dostępna pod adresem https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-272025-regarding-european-commission-draft_en.

⁽⁹⁵⁾ Decyzja wykonawcza Rady (UE) 2020/1745 z dnia 18 listopada 2020 r. w sprawie wprowadzenia w życie przepisów dorobku Schengen dotyczących ochrony danych oraz tymczasowego wprowadzenia w życie niektórych przepisów dorobku Schengen w Irlandii (Dz.U. L 393 z 23.11.2020, s. 3, ELI: http://data.europa.eu/eli/dec_impl/2020/1745/oj).

⁽⁹⁶⁾ Umowa zawarta przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotycząca włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen (Dz.U. L 176 z 10.7.1999, s. 36, ELI: [http://data.europa.eu/eli/agree_internation/1999/439\(1\)/oj](http://data.europa.eu/eli/agree_internation/1999/439(1)/oj)).

⁽⁹⁷⁾ Dz.U. L 53 z 27.2.2008, s. 52.

⁽⁹⁸⁾ Dz.U. L 160 z 18.6.2011, s. 21.

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Art. 4 decyzji wykonawczej (UE) 2021/1773 otrzymuje brzmienie:

„Artykuł 4

Niniejsza decyzja traci moc z dniem 27 grudnia 2031 r., chyba że okres jej stosowania zostanie przedłużony zgodnie z procedurą, o której mowa w art. 58 ust. 2 dyrektywy (UE) 2016/680.”.

Artykuł 2

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia 19 grudnia 2025 r.

W imieniu Komisji
Michael MCGRATH
Członek Komisji
